

Agent

Benutzerhandbuch

Version R9

Deutsch

März 19, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Agent-Übersicht

Agent

Mithilfe der Funktionen im Modul **Agent** können Benutzer Rechner-IDs erstellen, bearbeiten und löschen, das Aussehen des Agent-Symbols auf dem Rechner in der Systemablage ändern, die Häufigkeit der Agent-Anmeldung steuern und die Version der auf verwalteten Rechnern gespeicherten Agent-Software aktualisieren.

> **Hinweis:** Wenn Sie sich mit der Agent-Installation noch nicht auskennen, beziehen Sie sich auf die Schnellstartanleitung **Agent-Konfiguration und Verteilung** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/DE_RCtools_R9.pdf#zoom=70&navpanes=0)*.

Funktionen	Beschreibung
Agentstatus *(siehe 11)*	Zeigt aktive Benutzerkonten, IP-Adressen und die letzten Check-in-Zeiten an.
Agentprotokolle *(siehe 14)*	Zeigt die folgenden Protokolle an: • Agent-System- und Fehlermeldungen • Ausführung der Agent-Verfahren, ob erfolgreich oder fehlgeschlagen. • Von einem Benutzer vorgenommene Konfigurationsänderungen. • Senden/Empfangen von Daten für Anwendungen, die auf das Netzwerk zugreifen. • Anwendungs-, System- und Sicherheitsdaten im Ereignisprotokoll, die vom verwalteten Rechner erfasst wurden. • Alarmprotokoll • Fernsteuerungsprotokoll • Protokollüberwachung
Protokollhistorie *(siehe 15)*	Gibt an, wie lange die Protokolldaten gespeichert werden sollen.
Ereignisprotokolleinstellungen *(siehe 15)*	Gibt die in Ereignisprotokollen enthaltenen Protokolltypen und -kategorien an.
Agents verteilen *(siehe 19)*	Erstellt Agent-Installationspakete zum Installieren von Agents auf mehreren Rechnern.
Erstellen *(siehe 34)*	Erstellt Rechner-ID-Konten und/oder Installationspakete zum Installieren von Agents auf einzelnen Rechnern.
Löschen *(siehe 38)*	Löscht Rechner-ID-Konten.
Umbenennen *(siehe 39)*	Benennt vorhandene Rechner-ID-Konten um.
Gruppe ändern *(siehe 41)*	Weist Rechner einer anderen Rechnergruppe oder Untergruppe zu.
Einstellungen kopieren *(siehe 42)*	Kopiert Einstellungen von einem Rechnerkonto auf andere Rechnerkonten per Massenkopie.
Import/Export *(siehe 43)*	Importiert und exportiert Agent-Einstellungen, einschließlich geplanter Agent-Verfahren, zugewiesener Monitor-Sets und Ereignissätze als XML-Dateien.
Aussetzen *(siehe 44)*	Setzt alle Agent-Operationen, z. B. Agent-Verfahren,

	Monitoring und Patching aus, ohne die Einstellungen des Agents zu ändern.
Agent-Menü *(siehe 45)*	Passt das Agent-Menü auf verwalteten Rechnern an.
Check-in-Kontrolle *(siehe 48)*	Kontrolliert, wie oft Agents sich auf Agent-Rechnern anmelden.
Arbeitsverzeichnis *(siehe 51)*	Stellt einen Pfad zum Verzeichnis her, das vom Agent zum Speichern der Arbeitsdateien verwendet wird.
Profil bearbeiten *(siehe 52)*	Bearbeitet Rechnerkontodaten.
Portalzugriff *(siehe 54)*	Richtet Konten ein, um Rechnerbenutzern Fernzugriff auf ihre eigenen Rechner zu gestatten.
Anmeldedaten eingeben *(siehe 56)*	Stellt Anmeldedaten ein, die der Agent im Patch-Management, dem Verfahrensbefehl "Anmeldedaten verwenden", Endpoint Security und Desktop Management verwendet.
LAN-Cache *(siehe 58)*	Designiert einen Rechner so, dass er als Dateiquelle für andere Rechner auf dem gleichen LAN agiert.
LAN-Cache zuweisen *(siehe 60)*	Weist Rechner einem ausgewählten LAN-Cache-Rechner zu bzw. entfernt sie daraus.
Agent aktualisieren *(siehe 61)*	Aktualisiert die Agent-Software auf verwalteten Rechnern.
Dateizugriff *(siehe 62)*	Verhindert unberechtigten Zugriff auf Dateien auf verwalteten Rechnern durch Rogue-Anwendungen oder Benutzer.
Netzwerkzugriff *(siehe 64)*	Ermöglicht Ihnen, den Netzwerkzugriff auf Anwendungsbasis zu gestatten oder abzulehnen.
Anwendungsblocker *(siehe 67)*	Anwendungsblocker verhindert, dass beliebige Anwendungen auf einem verwalteten Rechner ausgeführt werden.

Agents

Die Verwaltung der Rechner über den VSA erfolgt durch Installieren eines Software-Clients auf einem verwalteten Rechner, der als ein **Agent** bezeichnet wird. Bei dem Agent handelt es sich um einen Systemdienst, bei dem der Benutzer nicht angemeldet sein muss, damit der Agent funktioniert, und der auch keinen Neustart erfordert, damit der Agent installiert werden kann. Der Agent ist konfigurierbar und kann für den Benutzer völlig unsichtbar sein. Der einzige Zweck des Agents ist es, die vom VSA-Benutzer angeforderten Aufgaben auszuführen. Nach der Installation:

- In der Systemablage des verwalteten Rechners wird ein Agent-Symbol, wie beispielsweise das Agent-Symbol angezeigt. Bei **Agent-Symbolen** *(siehe 3)* kann es sich um benutzerdefinierte Bilder handeln. Sie können jedoch auch ganz entfernt werden.
- Jedem installierten Agent wird eine eindeutige VSA Rechner-ID/Gruppen-ID/Organisation-ID zugewiesen. Rechner-IDs können automatisch bei der Installation des Agents oder einzeln vor der Installation des Agents erstellt werden.
- Jeder installierte Agent verbraucht eine der verfügbaren Agent-Lizenzen, die vom Service-Provider erworben wurden.
- Agents werden in der Regel über Pakete installiert, die mit Agent > **Agents bereitstellen** *(siehe 19)* im VSA erstellt werden.

- Auf einem Rechner können **mehrere Agents** *(siehe 29)* installiert werden, die jeweils auf einen anderen Server verweisen.
- Neben jeder Rechner-ID im VSA wird ein Check-in-Symbol angezeigt, das den Gesamtstatus des verwalteten Rechners angibt. Das Anmeldsymbol weist beispielsweise darauf hin, dass der Agent online und der Benutzer momentan angemeldet ist.
- Wenn Sie auf ein Anmeldesymbol klicken, wird eine einzelne Rechneroberfläche für den verwalteten Rechner namens Live-Connect angezeigt. **Live-Connect** bietet sofortigen Zugriff auf umfassende Daten und Tools, die Sie für das Arbeiten auf diesem spezifischen Rechner benötigen.
- Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt. Über das Agent-Schnellansichtsfenster können Sie ein Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten.

Agent-Symbole

Nachdem der Agent auf einem Rechner installiert wurde, wird er durch ein Symbol in der Systemablage des Rechners angezeigt. Dieses Symbol stellt die Schnittstelle des Rechnerbenutzers zum Agent dar. Das Symbol kann auf Wunsch des VSA-Benutzers über die Seite Agent > **Agent-Menü** *(siehe 45)* deaktiviert werden.

> **Hinweis:** Über System > Site-Anpassung können Sie Agent-Symbole vollständig anpassen. Siehe Benutzerdefinierte Agent-Symbole erstellen. Dies gilt auch für eindeutige Symbole für Apple- und Linux-Rechner.

Hintergrund des Agent-Symbols ist blau

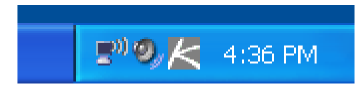
Wenn der Agent ausgeführt wird und **erfolgreich in den VSA eincheckt**, wird der Hintergrund des Agent-Symbols **blau** dargestellt.



> **Hinweis:** Durch Doppelklicken auf das Agent-Symbol wird die Willkommensseite für den Portal-Zugang angezeigt.

Hintergrund des Agent-Symbols ist grau

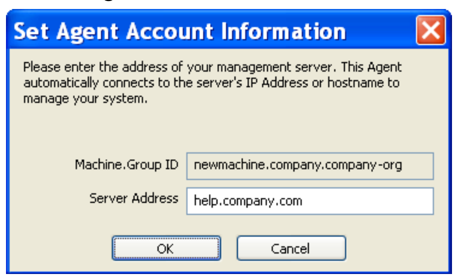
Ein ausgeführter Agent, der **nicht** in den VSA einchecken kann, wird als **graues Symbol** dargestellt. Dies zeigt an, dass entweder die Netzwerkverbindung ausgefallen ist oder der Agent an die falsche Adresse für den VSA verwiesen wird.



Bei einem grauen Agent-Symbol überprüfen Sie Folgendes:

1. Vergewissern Sie sich, dass dieser Rechner über Internetzugang verfügt.
2. Prüfen Sie, ob eine Firewall den **ausgehenden** Port blockiert, der vom Agent für die Verbindung mit dem VSA verwendet wird. Der Standard-Port ist 5721.
3. Vergewissern Sie sich, dass die Einstellungen für die **Check-in-Kontrolle** *(siehe 48)* für dieses Rechnerkonto korrekt sind.

4. Stellen Sie die VSA-Server-Adresse im Agent manuell ein, indem Sie mit der rechten Maustaste auf das Agentmenü klicken, **Konto einrichten...** auswählen und die richtige Adresse in das Formular eingeben.



Hintergrund des Agent-Symbols ist rot

Das Agent-Symbol wechselt zu **rot**, wenn ein Rechnerbenutzer die Fernsteuerung manuell deaktiviert. VSA-Benutzer verhindern die Fernsteuerung ihres Rechners durch andere Personen, indem sie mit der rechten Maustaste auf das Agent-Menü klicken und **Fernsteuerung deaktivieren** auswählen.



Hintergrund des Agent-Symbols blinkt abwechselnd weiß und blau

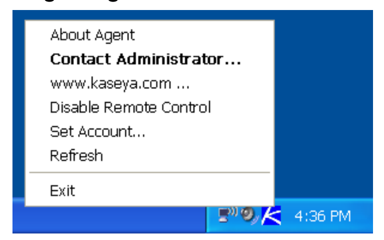
Das Agent-Symbol **blinkt** abwechselnd mit einem weißen Hintergrund und seinem normalen Hintergrund, wenn eine *Nachricht darauf wartet* gelesen zu werden. Die Nachricht wird durch Klicken auf das Symbol angezeigt.



> **Hinweis:** Eine Erläuterung dazu, wie das Senden von Nachrichten eingerichtet wird, finden Sie unter Fernsteuerung > Nachricht senden.

Optionen im Agent-Menü

Durch das Klicken mit der rechten Maustaste auf das Agent-Symbol wird ein Menü mit Optionen angezeigt, die dem Rechnerbenutzer zur Verfügung stehen.



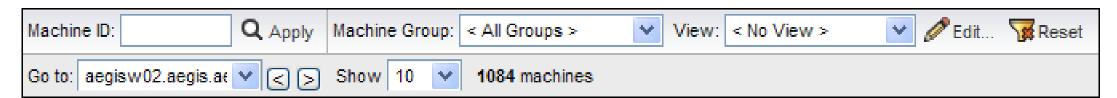
> **Hinweis:** Wie diese Optionen aktiviert oder deaktiviert werden, wird unter Agent > **Agent-Menü** *(siehe 45)* beschrieben.

Agent-Menü deaktivieren

VSA-Benutzer können das **Agent-Menü deaktivieren** *(siehe 45)* und das Symbol vom Desktop des Rechners entfernen.



Rechner-ID-/Rechnergruppen-Filter



Der Rechner-ID-/Rechnergruppen-ID-Filter steht auf allen Registerkarten und in allen Funktionen zur Verfügung. Mit seiner Hilfe können *Sie* anstelle eines Administrators die auf *allen* Funktionsseiten angezeigten Rechner beschränken. Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Nachdem Sie die Filterparameter angegeben haben, klicken Sie auf die Schaltfläche **Anwenden**, um die Filtereinstellungen auf *alle* Funktionsseiten anzuwenden. Der Rechner-ID-/Rechnergruppen-ID-Filter zeigt standardmäßig alle Rechner-IDs in `<All Groups>` an, die vom gegenwärtig angemeldeten VSA-Benutzer verwaltet werden.

> **Hinweis:** Selbst wenn ein VSA-Benutzer `<All Groups>` auswählt, werden nur Gruppen angezeigt, auf die dem VSA-Benutzer über System > Benutzersicherheit > Scopes Zugriff gewährt wurde.

- **Rechner-ID** – Beschränkt die Anzeige von Daten auf *allen* Funktionsseiten nach Rechner-ID-Zeichenfolge. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispiel: Durch die Eingabe der Zeichenfolge `ABC*` wird die Anzeige der Rechner-IDs auf allen Funktionsseiten auf Rechner-IDs beschränkt, die mit den Buchstaben `ABC` beginnen.

  Filtert die Anzeige von Rechnern nach Rechner-ID. Geben Sie den *Anfang* einer Zeichenfolge ein, um alle Rechner-IDs anzuzeigen, die mit dieser Zeichenfolge übereinstimmen. Fügen Sie ein Sternchen am Anfang einer Zeichenfolge ein, um alle Geräte zu finden, die mit der Zeichenfolge an einer beliebigen Stelle in der Rechner-ID übereinstimmen. Durch Eingabe der Zeichenfolge `*ABC` werden beispielsweise alle Rechner-IDs gesucht, die ABC an einer beliebigen Stelle in der Rechner-ID haben.
- **Anwenden** – Klicken Sie auf die Schaltfläche **Anwenden**, um die Filtereinstellungen auf alle Funktionsseiten anzuwenden.
- **Rechnergruppe** – Beschränkt die Anzeige von Daten auf allen Funktionsseiten nach Gruppen-ID oder Organisation. Eine Organisation mit nur *einer Rechnergruppe* zeigt nur die Rechnergruppe in der Drop-Down-Liste **Rechergruppe** an, nicht die Organisation. Organisationen mit *mehreren Rechnergruppen* zeigen die Organisation und alle Rechnergruppe für diese Organisation an. Dadurch kann die Organisation optional ausgewählt werden, um alle Rechnergruppen mit einzuschließen.
- **Anzeigen** – Ändern Sie die Ansichten, indem Sie eine andere Ansichtsdefinition auswählen. Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern.
- **Bearbeiten...** – Klicken Sie auf diese Option, um die Seite **Ansichtsdefinitionen** *(siehe 6)* anzuzeigen.
- **Zurücksetzen** – Löscht alle Filterungen.
- **Gehe zu** – Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.
- **Anzeigen** – Wählen Sie die Anzahl der Rechner-IDs aus, die auf jeder Seite angezeigt werden.
- **(Rechnerzahl)** – Zeigt die Rechnerzahl basierend auf den Filtereinstellungen an.

Ansichtdefinitionen

Rechner-ID-/Gruppen-ID-Filter > Bearbeiten...

Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Sie können mehrere Ansichten erstellen und benennen. Die Ansichtsfilterung wird auf *alle* Funktionsseiten angewendet, indem Sie eine **Ansicht** aus der Dropdown-Liste im Feld **Rechner-ID/Rechnergruppenfilter** *(siehe 5)* auswählen und auf das Symbol **Anwenden** klicken. Optionen werden nach Abschnitten organisiert, die nach Bedarf erweitert und reduziert werden können. Wenn eine Option eingestellt ist, bleibt der Abschnitt erweitert.

Kopfzeilenoptionen

- **Speichern** – Speichern Sie die ausgewählte Ansicht.
- **Speichern unter** – Speichern Sie die ausgewählte Ansicht unter einem neuen Namen.
- **Löschen** – Löschen Sie die ausgewählte Ansicht.
- **Ansicht auswählen** – Wählen Sie eine Ansicht aus.
- **Titel bearbeiten** – Bearbeiten Sie den Titel einer Ansicht.
- **Freigabe....** – Sie können eine Ansicht mit ausgewählten VSA-Benutzern und Benutzerrollen gemeinsam nutzen oder für alle VSA-Benutzer und Benutzerrollen freigeben.

So erstellen oder bearbeiten Sie eine neue Ansicht:

1. Klicken Sie auf die Schaltfläche **Bearbeiten...** rechts neben der Dropdown-Liste **Ansicht** im Feld für den Rechner-ID-/Gruppen-ID-Filter, um den Editor **Ansichtdefinitionen** zu öffnen.
2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie einen Namen für die neue Ansicht ein.
3. Geben Sie die gewünschten Filterspezifikationen ein.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Rechnerfilter

- **Rechner-ID einstellen** – Durch Aktivieren dieses Kontrollkästchens wird jeder Wert, der für das Feld **Rechner-ID** unter Rechner-ID-/Gruppen-ID-Filter eingestellt wurde, durch den hier eingegebenen Wert überschrieben. Das Feld Rechner-ID ist auf der Filterleiste Rechner-ID-/Gruppen-ID deaktiviert, um unabsichtliche Änderungen zu verhindern, wenn eine Ansicht angezeigt wird, bei der **Rechner-ID einrichten** ausgewählt ist.
- **Gruppen-ID einstellen** – Durch Aktivieren dieses Kontrollkästchens wird der **Gruppen-ID**-Filter im Feld für den Rechner-ID-/Gruppen-ID-Filter durch den hier eingegebenen Wert überschrieben. Das Feld Gruppen-ID ist auf der Filterleiste Rechner-ID-/Gruppen-ID deaktiviert, um unabsichtliche Änderungen zu verhindern, wenn eine Ansicht angezeigt wird, bei der **Gruppen-ID einstellen** ausgewählt ist.
- **Nur ausgewählte Rechner-IDs anzeigen** – Speichern Sie eine Ansicht zuerst, bevor Sie mit dieser Option Rechner-IDs auswählen. Sobald eine Ansicht gespeichert wurde, wird rechts von dieser Option ein Link **<N> Rechner ausgewählt** angezeigt. Klicken Sie auf diesen Link, um das Fenster **Sammlung definieren** anzuzeigen, in dem Sie mithilfe einer freien Sammlung von Rechner-IDs eine Ansicht erstellen können.

Rechnerstatus

- **Rechner zeigen, die in den letzen N Perioden online waren/nicht online waren/niemals online waren** – Aktivieren Sie dieses Kontrollkästchen, um diejenigen Rechner aufzulisten, deren Agents innerhalb des angegebenen Zeitraums am Kaseya Server angemeldet oder nicht angemeldet waren. Verwenden Sie die Option **nie**, um Rechner-ID-Vorlagenkonten zu filtern, da diese Konten sich nie anmelden.
- **Rechner zeigen, die ausgesetzt/nicht ausgesetzt sind** – Aktivieren Sie dieses Kontrollkästchen, um ausgesetzte oder nicht ausgesetzte Rechner aufzulisten.

- **Rechner zeigen, die in den letzten N Periode neu gestartet/nicht neu gestartet wurden** – Aktivieren Sie dieses Kontrollkästchen, um Rechner aufzulisten, die während des angegebenen Zeitraums keinen Neustart ausgeführt haben.
- **Rechner mit dem Anmeldestatus** – Aktivieren Sie dieses Kontrollkästchen, um Rechner mit dem ausgewählten Status der Anmeldedaten aufzulisten.
- **Connection Gateway-Filter** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Connection-Gateway mit dem angegebenen Filter übereinstimmt. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispielsweise entspricht `66.221.11.*` allen Connection-Gateway-Adressen von `66.221.11.1` bis `66.221.11.254`.
- **IP-Adressenfilter** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren IP-Adresse mit dem angegebenen Filter übereinstimmt. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispielsweise entspricht `66.221.11.*` allen IP-Adressen von `66.221.11.1` bis `66.221.11.254`.

Betriebssystem-Info

- **BS-Typ** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, die nach dem letzten Audit das ausgewählte Betriebssystem haben.
- **BS-Version** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, die nach dem letzten Audit die Betriebssystemzeichenfolge haben. Mit diesem Filter können Sie Rechner nach **Service Pack** identifizieren.

Skripting

- **Mit geplantem/nicht geplantem Agent-Verfahren** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, für die eine Ausführung des angegebenen Agen-Verfahrens geplant oder nicht geplant ist.

> **Hinweis:** Klicken Sie auf den Link **Agent-Verfahren auswählen**, um das Agent-Verfahren namentlich zu bezeichnen.

- **Letzter Ausführungsstatus erfolgreich/fehlgeschlagen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen das ausgewählte Agent-Verfahren bereits ausgeführt wurde. Wählen Sie das entsprechende Optionsfeld, um Rechner aufzulisten, auf denen das Agent-Verfahren erfolgreich ausgeführt wurde oder fehlschlug.
- **Agent-Verfahren wurde in den letzten N Tagen ausgeführt/nicht ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen das Agent-Verfahren während des angegebenen Zeitraums nicht ausgeführt wurde.

Anwendungen

- **Enthält Anwendung/Anwendung fehlt** – Aktivieren Sie dieses Kontrollkästchen, um unter Verwendung des angegebenen Filters nur die Rechner aufzulisten, auf denen eine Anwendung installiert oder nicht installiert ist. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Versionszeichenfolge ist > < = N** – Aktivieren Sie dieses Kontrollkästchen, um den Anwendungsfilter durch eine Versionsnummer größer als, kleiner als oder gleich einem angegebenen Wert noch weiter zu verfeinern.
- **Rechner mit folgendem installierten Modul anzeigen**
  - **Anti-Malware**
  - **Anti-Virus**

Zusatzmodule

- Filtern Sie Rechner basierend darauf, ob eine Client-Software für ausgewählte Zusatzmodule installiert ist.

Bezeichnung

- **Rechner mit allen oder einem beliebigen der folgenden Zeichen anzeigen** – Filtert Rechner über **alle** oder **beliebige** ausgewählte Zeichen.
- Eine Reihe von Schlüsseln in der lokalen Registrierung eines Rechners wird überprüft, um zu identifizieren, ob der Rechner als bestimmter Rechnertyp "gekennzeichnet" werden kann. Beispiele für Zeichen umfassen: `DNS Server`, `Domain Controller`, `POP3 Server`, `SMTP Server` und `SQL Server`. Die Kennzeichnung erfolgt automatisch. Jeder Agent-Rechner wird periodisch (in der Regel einmal pro Stunde) auf Konfigurationsänderungen überprüft, die die Kennzeichnung des Rechners beeinflussen könnten.

Patch-Verwaltung

- **Mitglieder der Patch-Richtlinie ein-/ausblenden** – Durch Aktivieren dieses Kontrollkästchens gemeinsam mit den Filtern Rechner-ID- und Gruppen-ID werden nur bestimmte Rechner aufgelistet, die zu einer spezifischen Patch-Richtlinie (**Einblenden**) oder nicht (**Ausblenden**) gehören.
- **Rechner ohne Patch-Scanergebnisse (nicht gescannt)** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, die nicht auf fehlende Patches gescannt wurden.
- **Rechner, auf denen mehr als oder gleich N Patches fehlen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen eine angegebene Anzahl von Microsoft-Patches *fehlt*.
- **Patch-Richtlinie verwenden** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen eine angegebene Anzahl von *bestätigten fehlenden* Microsoft-Patches fehlen.
- **Patch-Scan geplant/nicht geplant** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen ein Patch geplant ist oder nicht.
- **Letzter Ausführungsstatus erfolgreich/fehlgeschlagen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Patch-Scan erfolgreich war oder fehlschlug.
- **Patch-Scan wurde in den letzten <N> <Perioden> ausgeführt / nicht ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Patch-Scan innerhalb eines angegebenen Zeitraums ausgeführt oder nicht ausgeführt wurden.
- **Rechner mit 'Neustart anstehend' für Patch-Installationen** – Aktivieren Sie dieses Kontrollkästchen, um Rechner aufzulisten, auf denen ein Neustart für Patch-Installationen ansteht.
- **Rechner mit Patch-Testergebnissen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit dem ausgewählten Patch-Testergebnis aufzulisten.
- **Rechner mit automatischer Patch-Aktualisierungskonfiguration** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration Automatische Aktualisierung aufzulisten.
- **Rechner mit Konfiguration für Patch-Neustartaktion** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration für einen Neutstart aufzulisten.
- **Rechner mit Patch-Dateiquellenkonfiguration** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration für eine Patch-Dateiquelle aufzulisten.
- **Auf Rechnern fehlt ein spezifisches Patch (KB-Artikel-ID verwenden – nur Ziffern)** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, bei denen ein spezifisches Patch fehlt.
- **Rechner mit installiertem Patch (KB-Artikel-ID verwenden – nur Ziffern)** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner mit einem installierten Patch, das von KB-Artikel identifiziert wurde, aufzulisten.
- **Als Dateifreigabe verwendete Rechner** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, die als Dateifreigabe mit Dateiquelle konfiguriert wurden.
- **Rechner mit Dateifreigabe auf ausgewähltem Rechner** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit Dateifreigabe, die mit Dateiquelle konfiguriert wurde, auszuwählen.
- **Rechner mit Patch-Scan-Quelle auf online festgelegt, Offline-Scan wurde jedoch zuletzt ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Standard-Scan-Quelle auf online festgelegt ist, die jedoch zuletzt einen Offline-Scan ausgeführt haben.

- **Standard-Patch-Scan-Quelle Offline/Online.** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit einer Offline- oder Online-Standard-Patch-Scan-Quelle aufzulisten.
- **Automatische Windows-Aktualisierung aktiviert/deaktiviert** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, bei denen die automatische Windows-Aktualisierung aktiviert/deaktiviert ist.

Monitoring

- **Nur Rechner mit zugeordneten Monitor-Sets anzeigen <Monitor-Set auswählen>** – Wählen Sie diese Option, um alle Rechner, denen dieses Monitor-Set zugeordnet ist, aufzulisten.
- **Nur Rechner mit zugeordneten Monitor-Sets anzeigen <SNMP-Set auswählen>** – Wählen Sie diese Option, um alle Rechner, denen dieses Monitor-Set zugeordnet ist, aufzulisten.

Erweiterte Filterung

- **Erweiterter Datenfilter für Agents** – Aktivieren Sie dieses Kontrollkästchen und klicken Sie auf die Schaltfläche **Filter definieren...**, um die Ansicht mithilfe von **Filter-Gesamttabelle** *(siehe 9)* noch weiter zu verfeinern.

> **Warnung:** Sie müssen ein **Leerzeichen** eingeben, um den Operator in einem Filtereintrag von den Daten zu trennen. Der Filtereintrag `>= 500` enthält beispielsweise ein Leerzeichen genau nach dem Gleich-Zeichen.

Zusammengeführte Tabelle filtern

Rechner-ID-/Gruppen-ID-Filter > Bearbeiten... > Filter definieren...

Filter Gesamttabelle führt mehr als 75 Attribute für Agents und verwaltete Rechner auf, mit deren Hilfe eine Ansichtsdefinition unter Verwendung der Option **Erweiterte Filterung** *(siehe 9)* noch weiter verfeinert werden kann.

> **Hinweis:** Kollektionen stellen eine alternative Methode zur Auswahl von Rechner-IDs für eine **Ansichtsdefinition** *(siehe 6)* dar. Dabei kommt es nicht darauf an, ob sie irgendwelche Attribute gemeinsam nutzen.

Benutzerdefinierte Attribute

Über die Seite Audit > Systeminformation können Sie benutzerspezifische Attribute für **Filter Gesamttabelle** hinzufügen. Erstellen Sie dann Ansichtdefinitionen, die Rechner-IDs auswählen, die auf diesen benutzerdefinierten Attributen basieren.

Erweiterte Filterung

Erweiterte Filterung lässt Sie komplexe Suchvorgänge erstellen, um Daten auf nur die von Ihnen gewünschten Werte zu beschränken. Geben Sie Filterzeichenfolgen in dieselben Bearbeitungsfelder ein, in die Sie Filtertext eingeben.

> **Warnung:** Sie müssen ein **Leerzeichen** eingeben, um den Operator in einem Filtereintrag von den Daten zu trennen. Der Filtereintrag `>= 500` enthält beispielsweise ein Leerzeichen genau nach dem Gleich-Zeichen.

Erweiterte Filterung unterstützt die folgenden Operationen:

Leerzeichen

Schließen Sie die Zeichenfolge in Anführungszeichen ein, um darin nach Leerzeichen zu suchen.

Zum Beispiel: `"Microsoft Office*"` oder `"* Adobe *"`

Verschachtelte Operatoren

Alle Gleichungen werden von links nach rechts verarbeitet. Mit Klammern kann diese Standardeinstellung außer Kraft gesetzt werden.

Zum Beispiel: `(("* adobe " OR *a*) AND *c*) OR NOT *d* AND < m`

AND

Mit dem logischen Operator AND können Sie nach Daten suchen, die mehrere Werte enthalten müssen, aber an verschiedenen Stellen in der Zeichenfolge erscheinen können.

Zum Beispiel: `Microsoft* AND *Office*` gibt alle Elemente zurück, die sowohl Microsoft als auch Office in einer beliebigen Reihenfolge enthalten.

oder

Verwenden Sie den logischen Operator OR für die Suche nach Daten, die zwar mehrere Werte enthalten können, aber zumindest einen Wert enthalten müssen.

Zum Beispiel: `*Microsoft* OR *MS*` gibt alle Elemente zurück, die entweder Microsoft oder MS in beliebiger Reihenfolge enthalten.

NOT

Suchen Sie nach einer Zeichenfolge, die die Übereinstimmungsdaten nicht enthält.

Zum Beispiel: `NOT *Microsoft*` gibt alle Nicht-Microsoft-Anwendungen zurück.

Zum Beispiel: `NOT *Windows* AND NOT *update*` gibt alle Elemente zurück, die nicht entweder die Zeichenfolgen `Windows` oder `update` enthalten.

<, <= (Kleiner als oder kleiner als oder gleich)

Führt einen Zeichenfolgenvergleich aus, um alle Daten zurückzugeben, deren Wert weniger als der eingegebene Wert ist.

Zum Beispiel: `< G*` gibt alle Anwendungen aus, die mit einem Buchstaben kleiner als `G` beginnen.

Zum Beispiel: `< 3` gibt die Werte `2`, `21` und `287` zurück.

> **Hinweis:** Es kann auch nach Datumsangaben gesucht werden, aber dies muss im folgenden Format erfolgen: `YYYYMMDD HH:MM:SS` wobei `YYYY` das Jahr in 4-stelliger Schreibweise, `MM` den Monat in 2-stelliger Schreibweise (01 bis 12), `DD` den Tag in 2-stelliger Schreibweise (01-31), `HH` die Stunde in 2-stelliger Schreibweise (00-23), `MM` die Minute in 2-stelliger Schreibweise (00-59) und `SS` die Sekunde in 2-stelliger Schreibweise (00-59) angibt. `HH:MM:SS` ist optional. Datum und Uhrzeit werden durch eine Leerstelle getrennt.
>
> Zum Beispiel: `< 20040607 07:00:00` oder `< "20040607 07:00:00"` gibt alle Daten vor 7 Uhr am 7. Juni 2004 zurück. *Stellen Sie sicher, dass nach dem <-Operator ein Leerzeichen gesetzt ist.*

>, >= (Kleiner als oder kleiner als oder gleich)

Führt einen Zeichenfolgenvergleich aus, um alle Daten zurückzugeben, deren Wert mehr als der eingegebene Wert ist.

Zum Beispiel: `> G*` gibt alle Anwendungen aus, die mit einem Buchstaben größer als `G` beginnen.

Zum Beispiel: `> 3` gibt die Werte `3`, `3abc` und `30.129.101.76` zurück.

Agent-Version

Gibt alle Rechner mit einer angegebenen **Agent-Version** *(siehe 61)* zurück. Beispielsweise ist Agent-Version 6.2.1.1 als `6020101` angegeben.

Agentstatus

Agent > Rechnerstatus > Agent-Status

- *Agent-Status-Meldungen können über Monitoring > Benachrichtungen > Agent-Status definiert werden.*

Die Seite **Agent-Status** stellt eine Übersicht über eine Vielzahl von Agent-Daten bereit. Sie können alle Datenspalten selbst auswählen, um die Ansicht vollständig anzupassen. Spalten- und Filterauswahl gelten individuell für jeden VSA-Benutzer. Seitenzeilen können sortiert werden, indem Sie auf die Links der Spaltenüberschriften klicken.

- Über die Seite Audit > Systeminformation können benutzerdefinierten Datenspalten hinzugefüt werden. Nachdem sie hinzugefügt wurden, können Sie sie auf dieser Seite und im Bericht **Gesamttabelle** anzeigen.
- Verwenden Sie die Option **Rechner zeigen, die in den letzten N Perioden nicht online / niemals online waren** in **Ansichtdefinitionen** *(siehe 6)*, um die Anzeige von Rechner-IDs auf jeder Agent-Seite zu filtern.

Spalten auswählen...

Geben Sie die Datenspalten an und die Reihenfolge, in der sie angezeigt werden sollen.

Filter...

Klicken Sie auf **Filter...** , um eine **Filtergesamttabelle anzuzeigen.** Geben Sie Zeichenfolgen ein, um die Anzeige der Zeilen im Seitenbereich zu filtern. Wenn Sie beispielsweise nach der Rechner-ID suchen möchten, bei der "jsmith" angemeldet ist, geben Sie `jsmith` in das Bearbeitungsfeld neben **Aktueller Benutzer** ein. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

Filter zurücksetzen

Dies wird nur angezeigt, wenn ein erweiterter Filter eingestellt ist. Klicken Sie auf **Filter zurücksetzen**, um alle Zeichenfolgen zu löschen.

Spaltendefinitionen

Spalten werden in der standardmäßigen Reihenfolge beschrieben, in der sie auf dieser Seite angezeigt werden.

- **Rechner-D** – Rechner-ID-Bezeichnung, die im ganzen System verwendet wird
- **Aktueller Benutzer** – Anmeldename des gegebenenfalls aktuell am Rechner angemeldeten Benutzers
- **Letzter Neustartzeitpunkt** – Zeitpunkt des zuletzt bekannten Zeitpunkts des Rechnerneustarts
- **Letzter Check-in-Zeitpunkt** – Der letzte Zeitpunkt, an dem ein Rechner beim Kaseya Server eingecheckt war.
- **Gruppen-ID** – Gruppen-ID-Teil der Rechner-ID
- **Erster Anmeldezeitpunkt** – Der Zeitpunkt, zu dem ein Rechner sich zum ersten Mal am Kaseya Server angemeldet hat.
- **Zeitzone** – Vom Rechner verwendete Zeitzone
- **Computername** – Dem Rechner zugewiesener Computername.
- **Domäne/Arbeitsgruppe** – Arbeitsgruppe oder Domäne, zu der der Rechner gehört.
- **Arbeitsverzeichnis** – Das Verzeichnis auf dem verwalteten Rechner, das der Agent nutzt, um temporäre Dateien zu speichern.
- **DNS-Rechnername** – Vollständig qualifizierter DNS-Rechnername für den Rechner, der den Computernamen und den Domänennamen umfasst. Zum Beispiel: `jsmithxp.acme.com`. Der Rechnername wird nur angezeigt, wenn der Rechner Mitglied einer Arbeitsgruppe ist.

- **Agent-GUID** – Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
- **Betriebssystem** – Typ des Betriebssystems, das auf dem Rechner ausgeführt wird
- **BS-Version** – Versionsreihe des Betriebssystems.
- **IP-Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 4.
- **Subnetz-Maske** – Dem Rechner zugewiesenes Netzwerksubnetz.
- **Standard-Gateway** – Dem Rechner zugewiesener Standard-Gateway.
- **Connection-Gateway** – Die vom Kaseya Server erkannte IP-Adresse, wenn dieser Rechner sich anmeldet. Befindet sich der Rechner hinter einem DHCP-Server, ist dies die öffentliche IP-Adresse des Subnetzes.
- **Land** – Mit dem Connection-Gateway verknüpftes Land.
- **IPv6 Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 6.
- **MAC-Adresse** – MAC-Adresse der LAN-Karte, die zur Kommunikation mit dem Kaseya Server verwendet wird.
- **DNS-Server 1, 2** – IP-Adresse des dem Rechner zugewiesenen DNS-Servers.
- **DHCP-Server** – IP-Adresse des von diesem Rechner verwendeten DHCP-Servers.
- **Primärer/Sekundärer WINS** – WINS-Einstellungen.
- **CPU-Typ** – Prozessorversion und -modell.
- **CPU-Geschwindigkeit** – Taktgeschwindigkeit des Prozessors.
- **Prozessorzahl** – Anzahl der Prozessoren.
- **RAM-Größe** – MByte an RAM auf dem Rechner.
- **Agent-Version** – Versionsnummer des auf dem Rechner geladenen Kaseya-Agents.
- **Letzter angemeldeter Benutzer** – Anmeldename des zuletzt am Rechner angemeldeten Benutzers.
- **Portalzugriffsanmeldung** – Der einem Rechnerbenutzer zugewiesene Anmeldename zur Anmeldung am Kaseya Server.
- **Portalzugriff-Fernsteuerung** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und die Fernsteuerung *zu seinem eigenen Rechner von einem anderen Rechner aus* aktivieren kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Ticketing** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und Tickets eingeben kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Chat** – Dies ist aktiviert, wenn dieser Rechnerbenutzer Chat-Sitzungen mit einem VSA-Benutzer *einleiten* kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Primärer/Sekundärer KServer** – Vom Rechner verwendete IP-Adresse und Name zur Kommunikation mit dem Kaseya Server.
- **Intervall für Schnellanmeldung** – Zeiteinstellung für Schnellanmeldung in Sekunden.
- **Kontaktname** – Unter **Profil bearbeiten** *(siehe 52)* eingegebener Rechnerbenutzername.
- **Kontakt E-Mail** – E-Mail-Adresse wie in "Profil bearbeiten" eingegeben.
- **Kontakt-Telefon** – In "Profil bearbeiten" eingegebene Telefonnummer.
- **Kontakthinweise** – In "Profil bearbeiten" eingegebene Anmerkungen.
- **Hersteller** – Systemhersteller.
- **Produktname** – Produktname des Systems.
- **Systemversion** – Versionsnummer des Produkts.
- **System-Seriennummer** – Seriennummer des Systems.
- **Gehäuse-Seriennummer** – Seriennummer auf dem Gehäuse.
- **Gehäuse-Bestandsetikett** – Bestandsetikett auf dem Gehäuse.
- **Externe Busgeschwindigkeit** – Busgeschwindigkeit des Motherboards.
- **Max. Speichergröße** – Maximale Speichergröße des Motherboards.
- **Max. Speichersteckplätze** – Gesamtzahl der verfügbaren Speichermodulsteckplätze.
- **Gehäusehersteller** – Hersteller des Gehäuses.

- **Gehäusetyp** – Typ des Gehäuses.
- **Gehäuseversion** – Versionsnummer des Gehäuses.
- **Motherboard-Hersteller** – Hersteller des Motherboards.
- **Motherboard-Produkt-ID** – Produkt-ID des Motherboards
- **Motherboard-Version** – Versionsnummer des Motherboards.
- **Motherboard-Seriennummer** – Seriennummer des Motherboards.
- **Prozessorfamilie** – Installierter Prozessortyp.
- **Prozessorhersteller** – Hersteller des Prozessors.
- **Prozessorversion** – Versions-ID des Prozessors.
- **Max. CPU-Geschwindigkeit** – Maximal unterstützte Prozessorgeschwindigkeit.
- **Aktuelle CPU-Geschwindigkeit** – Aktuelle Geschwindigkeit des Prozessors
- **vPro-Hostname** – Von der vPro-Konfiguration eingestellter Name des vPro-fähigen Rechners.
- **vPro-Computername** – Vom Betriebssystem eingestellter Name des vPro-fähigen Rechners.
- **vPro-Modell** – Modell des vPro-fähigen Rechners.
- **vPro-Hersteller** – Hersteller des vPro-fähigen Rechners.
- **vPro-Version** – Version des vPro-fähigen Rechners.
- **vPro-Seriennummer** – Seriennummer des vPro-fähigen Rechners.
- **vPro-Bestandsnummer** – Identifikator zur Bestandsverwaltung, der dem vPro-fähigen Rechner zugewiesen wurde.
- **Hersteller des vPro-Motherboards** – Hersteller des Motherboards auf dem vPro-fähigen Rechner.
- **Produktname des vPro-Motherboards** – Produktname des Motherboards auf dem vPro-fähigen Rechner.
- **Version der vPro-Motherboards** – Versionsnummer des Motherboards auf dem vPro-fähigen Rechner.
- **Seriennummer der vPro-Motherboards** – Seriennummer des Motherboards auf dem vPro-fähigen Rechner.
- **Bestandsetikett der vPro-Motherboards** – Identifikator zur Bestandsverwaltung, der dem Motherboards des vPro-fähigen Rechners zugewiesen wurde.
- **Anbieter des vPro-Bios** – Anbieter des BIOS des vPro-fähigen Rechners.
- **Version des vPro-Bios** – Version des BIOS des vPro-fähigen Rechners.
- **Freigabedatum des vPro-Bios** – BIOS-Freigabedatum des vPro-fähigen Rechners

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Agentprotokolle

Agent > Rechnerstatus > Agent-Protokolle

Die Seite **Agent-Protokolle** zeigt Protokolldaten zu verwalteten Rechnern an. Für jede Art des Protokolls gibt es entsprechende Protokollberichte.

> **Hinweis:** Das System begrenzt die Anzahl der Protokolleinträge pro Protokolltyp pro Rechner automatisch auf 1.000. Sobald das Limit erreicht wird, werden die darüber liegenden Protokolleinträge archiviert (falls die Archivierung aktiviert ist) und aus dem System gelöscht. Die Archivoption wird in **Protokollverlauf** *(siehe 15)* eingestellt.

Rechner-ID

Klicken Sie auf den Hyperlink einer Rechner-ID, um alle Protokolle dieser Rechner-ID zu listen.

Protokoll auswählen

Wählen Sie ein Protokoll aus der Dropdown-Liste **Protokoll auswählen**. Es gibt folgende Protokollarten:

- **Alarmprotokoll** – Listet alle ausgelösten Alarme für den ausgewählten Rechner auf.
- **Monitor-Aktionsprotokoll** – Das Protokoll der Meldungsbedingungen sowie die entsprechenden Aktionen, die als Antwort darauf ergriffen wurden.

  > **Hinweis:** Ein Zählerwert von -008 in den Kontrollprotokollen gibt an, dass der Monitorset keine Daten zurückgibt. Überprüfen Sie, dass der `Performance Logs & Alerts`-Dienst in Windows ausgeführt wird. Dies ist eine Voraussetzung für die Überwachung der Leistungszähler.

- **Agent-Protokoll** – Zeigt ein Protokoll der Agent-, System- und Fehlermeldungen an.
- **Konfigurationsänderungen** – Zeigt Änderungen an den VSA-Einstellungen für den ausgewählten Rechner an.
- **Netzwerkstatistiken** – Zeigt ein Protokoll vpn Daten senden/empfangen für Netzwerkanwendungen an.

  > **Hinweis:** Für dieses Protokoll muss der Treiber Audit > **Netzwerkzugriff** *(siehe 64)* aktiviert sein. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. Er ist standardmäßig *deaktiviert*.

- **Ereignisprotokolle** – Zeigt die von Windows gesammelten Ereignisprotokolldaten an. Dies ist nicht für Win9x verfügbar. In der Dropdown-Liste des Ereignisprotokolls werden nur Ereignisprotokolle angezeigt, die auf den ausgewählten Rechner zutreffen. Ein gibt einen als Warnung klassifizierten Protokolleintrag an. Ein gibt einen als Fehler klassifizierten Protokolleintrag an. Ein gibt einen als Information klassifizierten Protokolleintrag an.

  Ein Monitorassistent--Symbol wird neben dem Ereignisprotokolleintrag im VSA und in **Live Connect** angezeigt. Durch Klicken auf das Monitor-Assistent-Symbol eines Protokolleintrags wird ein Assistent angezeigt. Der Assistent ermöglicht Ihnen auf Basis dieses Protokolleintrags ein neues Kriterium für den Ereignissatz zu erstellen. Das neue Ereignissatz-Kriterium kann zu jedem neuen oder bestehenden Ereignissatz hinzugefügt werden. Der neue oder geänderte Ereignissatz wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehender Ereignissatz geändert, so sind alle Rechner davon betroffen, denen dieser Ereignissatz zugeordnet ist. Das Monitorassistent-Symbol wird angezeigt in:

  - Agent>Agent-Protokolle
  - Live Connect > Ereignisanzeige
  - Live Connect > Agent-Daten > Ereignisprotokoll

Unter Monitor > Ereignisprotokoll-Meldungen finden Sie eine Beschreibung der jeweiligen Felder, die im Assistenten angezeigt werden.

- **Agent-Verfahrensprotokoll** – Protokoll der erfolgreichen/fehlgeschlagenen Agent-Verfahren.
- **Legacy-Remote-Control-Protokoll** – Zeigt ein Protokoll der Remote-Control-Sitzungen unter Verwendung des Moduls Remote Control an.
- **Kaseya-Remote-Control-Protokoll** – Zeigt ein Protokoll der Remote-Control-Sitzungen unter Verwendung von Kaseya Remote Control an.
- **Protokoll-Monitoring** – Zeigt Einträge des Protokoll-Monitoring an.

Ereignisse pro Seite

Wählen Sie die Anzahl der Zeilen aus, die pro Seite angezeigt werden sollen.

Startdatum/ Enddatum/Aktualisieren

Wählen Sie einen Datumsbereich zum Filtern der Protokolldaten aus und klicken Sie dann auf die Schaltfläche **Aktualisieren**.

Filter...

Gilt nur für `Ereignisprotokolle`. Klicken Sie auf **Filter...**, um die Menge der angezeigten Daten einzuschränken. Für jede angezeigte Ereigniskategorie und Datenspalte kann ein anderer erweiterter Filter angegeben werden.

Ereignisprotokollfilter anwenden

Gilt nur für `Ereignisprotokolle`. Der Ereignisprotokollfilter enthält Optionen, die über die Schaltfläche **Filter...** definiert werden. Wenn **Ereignisprotokollfilter anwenden** aktiviert ist, wird die Filterung angewendet.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Protokollhistorie

Agent > Rechnerstatus > Protokollverlauf

Auf der Seite **Protokollverlauf** wird die Anzahl der Tage festgelegt, für die Protokolldaten auf einer Pro-Protokoll-Basis für jede Rechner-ID in der Datenbank gespeichert werden. Protokolldaten werden über **Agent-Protokolle** *(siehe 14)* angezeigt oder mit Info Center > Reporting > Protokolle ausgedruckt. Außerdem wird auf dieser Seite festgelegt, ob Agent-Protokolldaten später in Textdateien in einem Netzwerkverzeichnis archiviert werden. Das Verzeichnis wird mit System > Serververwaltung > Konfigurieren bezeichnet. Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.

- **Protokolleinstellungen** können auch mithilfe der Registerkarte **Agent-Einstellungen** von Live-Connect > Agentdaten oder der Seite Rechnerübersicht gepflegt werden.
- System > Systemeinstellungen > Check-in-Richtlinie kann die Anzahl der Tage einschränken, für die Benutzer die Protokolleinträge behalten können, um eine unnötige Last auf den Servern zu vermeiden, auf denen der Kaseya Server-Dienst ausgeführt wird.
- Diese Einstellungen werden standardmäßig aus dem Agent-Installationspaket übernommen. Agent-Installationspakete werden über Agent > **Agent einrichten** *(siehe 19)* erstellt.

Größenanforderungen der Datenbank schätzen

Je mehr Daten Sie protokollieren, desto größer wird die Datenbank. Die Größenanforderungen der

Datenbank können unterschiedlich sein. Es kommt auf die Anzahl der bereitgestellten Agents und die aktivierte Protokollierungsstufe an. Um die Größenanforderungen der Datenbank für Protokolldaten zu schätzen, erstellen Sie einen Auszug der `nteventlog`-Tabelle der Datenbank. Legen Sie fest, wie viele Daten pro Tag protokolliert werden und schätzen Sie dann anhand dieses Werts den zusätzlichen Speicherplatz ein, der für ein längeres Speichern der Protokolle erforderlich ist.

Anzahl Tage festlegen, die Protokolleinträge aufbewahrt werden sollen. Markieren, um Einträge in Datei zu archivieren

Legen Sie die Anzahl der Tage fest, für die Protokolleinträge für jede Art von Protokoll aufbewahrt werden sollen. Aktivieren Sie das Kontrollkästchen für jedes Protokoll, um Protokolldateien nach ihrem Enddatum zu archivieren.

- **Konfigurationsänderungen** – Protokoll der von jedem Benutzer vorgenommenen Konfigurationsänderungen.
- **Netzwerkstatistiken** – Protokoll der ein- und ausgehenden Paketzahlinformationen und der Anwendung oder des Prozesses, die/der solche Pakete überträgt und/oder empfängt. Die Informationen können im Detail über Agent > **Agent-Protokolle** *(siehe 14)* > Netzwerk-Statistik angezeigt werden.
- **Agent-Verfahrensprotokoll** – Protokoll der erfolgreichen/fehlgeschlagenen Agent-Verfahren.
- **Legacy-Remote-Control-Protokoll** – Zeigt ein Protokoll der Remote-Control-Sitzungen unter Verwendung des Moduls Remote Control an.
- **Kaseya-Remote-Control-Protokoll** – Zeigt ein Protokoll der Remote-Control-Sitzungen unter Verwendung von Kaseya Remote Control an.
- **Alarmprotokoll** – Protokoll aller ausgegebener Alarme.
- **Monitoring-Aktion** – Protokoll der aufgetretenen Meldungsbedingungen sowie die entsprechenden Aktionen, die als Reaktion darauf ergriffen wurden.
- **SYS-Protokoll** – Das Protokoll "Protokollüberwachung".
- **Agent-Betriebszeitprotokoll** – Protokolliert den Betriebsverlauf von Agents. Anzahl der Tage muss auf 1 oder höher gesetzt sein, um eine genaue Zeiterfassung des letzten Neustarts zu erhalten. Siehe **Erfassen der letzten Neustartzeiten für den Agent** *(https://helpdesk.kaseya.com/entries/35994418)* und **Schaltfläche "Jetzt neu starten" bleibt und/oder Endbenutzer meldet fortlaufenden Reboot-Nag nach Neustart** *(https://helpdesk.kaseya.com/entries/33901207)*.

> **Hinweis:** Alle oben aufgelisteten Agent-Protokollarchive werden in dem vom Feld System > Serververwaltung > Konfigurieren > **Pfad des Protokolldateiarchivs** angegebenen Verzeichnis gespeichert.

Festlegen, wie viele Tage die Monitor-Protokolle für alle Rechner aufbewahrt werden sollen

Die folgenden Monitoring-Protokolleinstellungen werden systemweit angewendet.

- **Ereignisprotokoll** – Protokoll aller Ereignisse. Die erfassten Ereignisse werden detaillierter über Agent > **Ereignisprotokolleinstellungen** *(siehe 17)* angegeben.
- **Monitoring-Protokoll** – Protokoll der von Monitor-Sets erfassten Daten
- **SNMP-Protokoll** – Protokoll aller von SNMP-Sets erfassten Daten.
- **Agent-Protokoll** – Protokoll der Agent-, System- und Fehlermeldungen

> **Hinweis:** Die Protokollarchive der Monitoring-Daten auf der Seite "Agent > **Protokollhistorie** *(siehe 15)*" werden im Verzeichnis `<KaseyaRoot>\UserProfiles\@dbBackup` gespeichert. Damit soll die Leistung von Systemen verbessert werden, bei denen sich die Datenbank auf einem anderen Server befindet. Alle anderen Agent-Protokollarchive werden in dem im Feld "System > Konfigurieren > **Pfad des Protokolldateiarchivs**" angegebenen Verzeichnis gespeichert.

Alle Tage festlegen

Klicken Sie auf **Alle Tage festlegen**, um alle Tag-Felder auf denselben Wert einzustellen.

Alle Archive auswählen/Alle Archive abwählen

Klicken Sie auf den Link **Alle Archive auswählen**, um alle Archiv-Kontrollkästchen auf der Seite zu markieren. Klicken Sie auf den Link **Alle Archive abwählen**, um alle Archiv-Kontrollkästchen auf der Seite zu deaktivieren.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um ausgewählte Rechner-IDs mit AgentProtokolleinstellungen zu aktualisieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Ereignisprotokolleinstellungen

Agent > Rechnerstatus > Ereignisprotokolleinstellungen

Die Seite **Ereignisprotokolleinstellungen** gibt die Kombination von Ereignisprotokoll-Typen und -Kategorien an, die vom VSA erfasst werden.

> **Hinweis:** Meldungen können mit Monitoring > Ereignisprotokollmeldungen separat für Ereignisse angegeben werden. **Ereignisprotokollmeldungen werden auch noch erstellt, wenn Ereignisprotokolle nicht vom VSA erfasst werden.**

So legen Sie **Ereignisprotokolleinstellungen** fest:

1. Klicken Sie im Listenfeld **Ereignisprotokolltypen** auf einen Ereignisprotokolltyp. Halten Sie die [Strg]-Taste gedrückt, um mehrere Ereignisprotokolltypen auszuwählen.
2. Klicken Sie auf **Hinzufügen>**, um Ereignisprotokolltypen zum Listenfeld **Zugewiesene Ereignistypen** hinzuzufügen. Klicken Sie auf **<< Entfernen** oder **<< Alle entfernen**, um Ereignisprotokolltypen aus dem Listenfeld **Zugewiesene Ereignistypen** zu entfernen.
3. Markieren Sie eine oder mehrere Ereigniskategorien: **Fehler, Warnung, Informationen, Audit erfolgreich, Audit fehlgeschlagen, Kritisch, Verbose.**
4. Wählen Sie eine oder mehrere Rechner-IDs aus.

5. Klicken Sie auf **Aktualisieren** oder **Ersetzen**, um diese Einstellungen auf ausgewählte Rechner-IDs anzuwenden.

Globale Ereignisprotokolllisten

Jeder Agent verarbeitet zwar alle Ereignisse, die auf einer "Blacklist" aufgeführten Ereignisse werden jedoch *nicht* auf den VSA-Server hochgeladen. Es gibt zwei "Blacklists". Eine wird periodisch von Kaseya aktualisiert und trägt die Bezeichnung `EvLogBlkList.xml.`. Die zweite mit dem Namen `EvLogBlkListEx.xml` kann vom Dienstanbieter verwaltet werden und wird nicht von Kaseya aktualisiert. Beide befinden sich im Verzeichnis `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles`. Die Alarmermittlung und -verarbeitung werden fortgesetzt, ungeachtet dessen, ob sich die Einträge in der Erfassungs-Blacklist befinden oder nicht.

Fluterkennung

Wenn 1000 Ereignisse (ohne Zählung der Blacklist-Ereignisse) von einem Agent *innerhalb einer Stunde* auf den Kaseya Server hochgeladen werden, wird die weitere Erfassung von Ereignissen dieses Protokolltyps für den Rest der Stunde angehalten. Ein neues Ereignis wird in das Ereignisprotokoll eingefügt, um die Aussetzung der Erfassung zu verzeichnen. An Ende der Stunde wird die Erfassung automatisch wieder aufgenommen. Dies verhindert, dass der Kaseya Server von kurzfristigen Schwerlasten überschwemmt wird. Die Alarmermittlung und -verarbeitung wird ungeachtet einer ausgesetzten Erfassung fortgesetzt.

Aktualisieren

Fügt die im Listenfeld **Zugewiesene Ereignistypen** aufgeführten Ereignisprotokolltypen zum Satz der Ereignisprotokolltypen hinzu, die bereits ausgewählten Rechner-IDs zugewiesen wurden.

Ersetzen

Ersetzt alle den ausgewählten Rechner-IDs zugewiesenen Ereignisprotokolltypen durch die Ereignisprotokolltypen, die in der Liste **Zugewiesene Ereignistypen** aufgeführt werden.

Alle löschen

Löscht alle Ereignisprotokolltypen, die ausgewählten Rechner-IDs zugewiesen wurden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System >

Benutzersicherheit > Scopes anzuzeigen.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol ✗, um diesen Datensatz zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Rechner-ID, um automatisch Kopfzeilenparameter einzustellen, die mit denjenigen der ausgewählten Rechner-ID übereinstimmen.

Zugewiesene Kategorien

Dies sind die Ereigniskategorien, die vom VSA für diese Rechner-ID und das Ereignisprotokoll gespeichert werden:

- **F**ehler
- **W**arnung
- **I**nformationen
- **A**udit erfolgreich
- **A**udit fehlgeschlagen
- **K**ritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
- **V**erbose – betrifft nur Vista, Windows 7 und Windows Server 2008

Agents verteilen

Agent > Agents installieren > Agents bereitstellen

Auf der Seite **Agent bereitstellen** wird ein Agent-Installationspaket erstellt und auf *mehreren* Rechnern bereitgestellt.

Agent-Installationspakete

Agents werden auf verwalteten Rechnern über ein **Agent-Installationspaket** installiert. Ein Agent-Installationspaket enthält alle Einstellungen, mit denen ein Agent auf einem Zielrechner funktionieren soll.

Die Seite Agent > **Agent bereitstellen** zeigt die in Ihrem VSA verfügbaren Agent-Installationspakete an. Ein `Default Install`-Paket wird mit dem VSA bereitgestellt. Es werden möglicherweise andere Agent-Installationspakete angezeigt, die bereits erstellt und auf dieser Seite aufgelistet wurden.

Ein Agent-Installationspaket wird über den Assistenten **Automatische Kontenerstellung konfigurieren** erstellt. Der Assistent kopiert Agent-Einstellungen von einer *vorhandenen* Rechner-ID oder Rechner-ID-Vorlage und erstellt ein Installationspaket mit der Bezeichnung `KcsSetup.`. Alle Einstellungen und ausstehenden Agent-Verfahren für die Rechner-ID, von der Sie kopieren – abgesehen von Rechner-ID, Gruppen-ID und Organisations-ID – werden auf jede neue Rechner-ID angewendet, die mit dem Paket erstellt wird.

> **Hinweis:** Weitere Hinweise finden Sie in der PDF-Schnellstartanleitung **Agent-Konfiguration und Verteilung** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/DE_agentdeployment_R9.pdf#zoom=70&navpanes=0).*

Weitere Themen

- **Agent-Installationspaket erstellen** *(siehe 20)*
- **Manuelle Installation des Agents** *(siehe 21)*
- **Automatisieren der Agent-Installation** *(siehe 23)*
- **Agent-Installationspakete pflegen** *(siehe 24)*
- **Agent-Einstellungen konfigurieren** *(siehe 24)*

- **Befehlszeilenschalter für Agent-Installation** *(siehe 27)*
- **Probleme und Fehler bei der Installation** *(siehe 29)*
- **Mehrere Agents installieren** *(siehe 29)*
- **Installation von Linux Agents** *(siehe 31)*
- **Unterstützte Linux Funktionen** *(siehe 33)*
- **Unterstützte Apple-Funktionen** *(siehe 33)*

Aktionen

- **Hier klicken, um den Standard-Agent herunterzuladen** – Klicken Sie auf diesen Link, um das Standardpaket des aktuellen VSA-Benutzers direkt von dieser Seite herunterzuladen.
- **Benutzer können Agents herunterladen von** – Fügen Sie diesen Hyperlink in eine E-Mail-Nachricht ein. Die *eindeutige ID-Nummer* stellt sicher, dass beim Klicken auf den Link in der E-Mail-Nachricht das Standard-Installationspaket ausgewählt und heruntergeladen wird. Stellen Sie ein anderes Installationspaket als Standard ein, um den Link für dieses Installationspaket anzuzeigen.
- **Pakete aller Administratoren verwalten** – Aktivieren Sie dieses Kontrollkästchen, um alle von allen VSA-Benutzern erstellten Pakete anzuzeigen. Nachdem ein verborgenes Paket angezeigt wurde, können Sie es verwenden oder öffentlich machen. Diese Option wird nur für Masterrollenbenutzer angezeigt.

Tabellenspalten

- **Standard einrichten** – Geben Sie Ihr eigenes Standard-Installationspaket an, indem Sie das Optionsfeld links neben dem Paketnamen in der Spalte **Standard einrichten** auswählen.
- **Löschen-Symbol** – Klicken Sie auf das Löschen-Symbol, um ein Paket aus dem Seitenbereich zu entfernen. Wenn das Paket von Ihnen erstellt wurde, wird es ebenfalls aus dem System gelöscht und aus allen Listen der VSA-Benutzer entfernt.
- **Bearbeitungssymbol** – Klicken Sie auf das Bearbeitungssymbol neben einem Paket, um mithilfe des Assistenten **Automatische Kontenerstellung konfigurieren** die Parameter für dieses Paket zu ändern.
- **Paketname** – Listet den Namen des Pakets auf.
- **Öffentliches Paket** – Die Zeilen in öffentlichen Paketen werden mit einem braunen Hintergrund angezeigt. Die Zeilen in privaten Paketen werden mit einem grauen Hintergrund angezeigt.
- **Gemeinsam nutzen** – Klicken Sie auf **Gemeinsam nutzen**, damit Sie ein privates Paket mit anderen Benutzern und Benutzerrollen gemeinsam nutzen oder das Paket öffentlich machen können.
- **Liste in dl.asp** – Klicken Sie auf den Link **dl.asp** im Spaltenkopf, um die Webseite anzuzeigen, die Rechnerbenutzer beim Installieren eines Agents auf ihrem Rechner sehen. Aktivieren Sie ein Kontrollkästchen in dieser Spalte, um ihr Paket in die Liste der verfügbaren Download-Pakete auf der Seite **dl.asp** aufzunehmen.
- **Beschreibung** – Zeigt die Beschreibung des Pakets an.

Agent-Installationspaket erstellen

Klicken Sie auf der Seite Agent > **Agents bereitstellen** *(siehe 19)* auf **Paket erstellen**, um den Assistenten **Automatische Kontenerstellung konfigurieren** zu starten. Der Assistent ist ein Verfahren mit 7 Schritten.

1. Definieren Sie Regeln für die Benennung der Rechner-ID.
   - Fordern Sie den Benutzer auf, eine Rechner-ID einzugeben.
   - Verwenden Sie den Rechnernamen als Rechner-ID.
   - Stellen Sie den Benutzernamen des gegenwärtig angemeldeten Benutzers als Rechner-ID ein.
   - Geben Sie eine feste Rechner-ID für dieses Installationspaket an.

2. Definieren Sie Regeln für die Benennung der Gruppen-ID.
   - **Bestehende Gruppe** – Wählen Sie eine vorhandene Gruppen-ID aus einer Dropdown-Liste aus.
   - **Domänen-Name** – Verwenden Sie den Domänen-Namen des Benutzers.
   - **Neue Gruppe** – Geben Sie eine neue Gruppen-ID an. Diese Option wird nur für Masterrollenbenutzer angezeigt.
   - **Benutzer auffordern** – Der Benutzer wird zur Eingabe einer Gruppen-ID aufgefordert. Diese Option wird nur für Masterrollenbenutzer angezeigt.
3. Geben Sie **Befehlszeilenschalter** *(siehe 27)* für das Agent-Installationspaket an, einschließlich der Möglichkeit, die Installation automatisch ohne Taskleisten oder Dialogfelder auszuführen.
4. Geben Sie die Rechner-ID an, von der Einstellungen und anstehende Agent-Verfahren kopiert werden sollen. Sämtliche Einstellungen und anstehenden Agent-Verfahren (außer der Rechner-ID, Gruppen-ID und Organisations-ID) werden auf jede neue, mit dem Paket erstellte Rechner-ID angewendet.

> **Hinweis:** Die Anweisung `Copy settings from unknown.root.unnamed if nothing selected` basiert auf der Rechner-ID oder -Vorlage, die vom Standard-Installationspaket ausgewählt wurde.

5. Wählen Sie das Betriebssystem aus, für das Sie das Installationspaket erstellen: `Automatically choose OS of downloading computer:` `Windows`, `Macintosh` oder `Linux.`
6. Binden Sie optional die Anmeldedaten eines Benutzers an das Installationspaket. Füllen Sie das Formular **Administratoranmeldedaten** aus, um die Benutzerrechte sicher an das Installationsformular zu binden.
   - Benutzer ohne Administratorrechte können das Installationspaket erfolgreich installieren, ohne Administrator-Anmeldedaten eingeben zu müssen.
   - Wenn die Administrator-Anmeldedaten leer gelassen werden und der Benutzer keine Administratorrechte zum Installieren von Software hat, wird er während der Installation vom Installationspaket zur Eingabe von Administrator-Anmeldedaten aufgefordert. **Falls das Paket automatisch installiert wird, schlägt `KcsSetup` fehl, ohne dass die Gründe hierfür in irgendwelchen Dialogmeldungen angezeigt werden.**

> **Administratoranmeldedaten** – Gegebenenfalls kann ein Agent-Installationspaket erstellt werden, das Anmeldedaten eines Administrators für den Zugriff auf ein Kundennetzwerk enthält. Anmeldedaten sind nur erforderlich, wenn Benutzer Pakete auf Rechnern installieren und keinen Administratorzugriff auf ihr Netzwerk haben. Die Anmeldedaten des Administrators sind verschlüsselt, niemals als Klartext verfügbar und an das Installationspaket gebunden.

7. Benennen Sie das Installationspaket, damit später leicht darauf verwiesen werden kann. Dieser Name wird auf der Seite **Agents bereitstellen** und der Download-Seite `dl.asp` angezeigt.

Manuelle Installation des Agents

Installationspakete von der Seite "Agent bereitstellen" manuell herunterladen

Auf der Seite **Agent bereitstellen** werden drei Arten von Links zum Herunterladen von Agent-Installationspaketen zur Verfügung gestellt:

- **Klicken Sie auf den Link "Standard-Agent herunterladen"** – Jeder Benutzer besitzt sein eigenes Standard-Agent-Installationspaket. Klicken Sie auf diesen Link, um Ihren eigenen Benutzer-Standard-Agent herunterzuladen.
- **Klicken Sie auf den Link "Paket"** – Die vollständige Liste von verfügbaren Agent-Installationspaketen wird auf der Seite **Agents bereitstellen** angezeigt. Klicken sie auf einen dieser Links, um das Agent-Installationspaket herunterzuladen.

- **Klicken Sie auf den Link "dl.asp"** – Auf der `dl.asp`-Webseite werden alle öffentlich verfügbaren Agent-Installationspakete aufgelistet. Klicken Sie auf ein beliebiges Paket auf der "dl.asp"-Webseite, um es herunterzuladen.

Mit jeder dieser Methoden wird die gleiche `KcsSetup`-Datei zum Installieren des Agents heruntergeladen.

Installieren eines Agents mithilfe der dl.asp Page

Die folgende ist die schnellste Methode für die manuelle Installation eines Agents.

1. Melden Sie sich bei dem Rechner an, auf dem der Agent installiert werden soll.
2. Geben Sie die folgende URL in den Browser des Rechners ein:
   `http://<YourVSAaddress>/dl.asp`
3. Klicken Sie auf das Paket `Default Install`, um die Installation des Agent auf dem Rechner zu starten.
   - Falls noch andere Installationspakete aufgeführt sind, wählen Sie Ihr bevorzugtes Paket aus.
   - Im Verlauf der Installation müssen Sie möglicherweise eine Bestätigung eingeben, damit der Vorgang abgeschlossen werden kann.
4. Melden Sie sich bei VSA an:
   `http://<YourVSAaddress>`
5. Wählen Sie im VSA die Seite Agent > **Agent-Status** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#250.htm)*.

Auf der Seite sollte jetzt ein neues Rechnerkonto für den soeben erstellten Agent angezeigt werden.

Ausführen des Agent-Installationspakets auf dem Endpunktrechner

Benutzer können das `KcsSetup`-Installationsprogramm auf dem Endpunktrechner auf folgende Arten ausführen:

- *Fenster*
  - Doppelklicken Sie auf `KcsSetup`, um es zu starten.
  - Öffnen Sie ein **Befehlszeilenfenster** und geben Sie `KcsSetup` gefolgt von jeden gewünschten **Befehlszeilenschaltern** *(siehe 27)* ein.
  - Wählen Sie **Ausführen...** im **Windows-Startmenü** und geben Sie `KcsSetup` gefolgt von jeden gewünschten Befehlszeilenschaltern ein.
- *Apple und Linux*
  - Doppelklicken Sie auf `KcsSetup`, um es zu starten.
  - Der vollständige Dateiname für ein Macintosh-Agent-Installationspaket lautet `KcsSetup.app`. `KcsSetup.app` wird als ein `KcsSetup.zip` heruntergeladen, was `KcsSetup.app` innerhalb eines Ordners mit dem Titel `Agent` enthält. Klicken Sie auf die `KcsSetup.zip`-Datei, um sie zu erweitern, klicken Sie dann auf den Ordner `Agent` und anschließend auf die Datei `KcsSetup.app`, um diese auszuführen.

> **Hinweis:** Bei Apple können **Befehlszeilenschalter** *(siehe 27)* nur für die Erstellung des Agent-Installationspaketes verwenden werden.
>
> **Hinweis:** Bei Linux erhalten Sie weitere Informationen unter **Installation von Linux Agents** *(siehe 31)*.

Neuinstallieren von Agents

Auf der Seite **Erstellen** *(siehe 34)* können Sie einen Agent für ein vorhandenes Rechner-ID-Konto neu installieren.

Automatisieren der Agent-Installation

Mithilfe der folgenden Methoden können Sie die Installation von Agent-Installationspaketen automatisieren:

Login

- **Windows** – Richten Sie ein **NT-Anmelde**verfahren ein, um das Installationspaket jedes Mal auszuführen, wenn sich ein Benutzer am Netzwerk anmeldet. Siehe Systemveraussetzungen.
- **Apple** – Richten Sie ein **Apple OS X Login Hook-Verfahren** ein, um das Installationspaket jedes Mal auszuführen, wenn sich ein Benutzer am Netzwerk anmeldet. Siehe Kaseya KB-Artikel **HT2420** *(http://support.apple.com/kb/HT2420)*.

Verfahren

1. Erstellen Sie das Bereitstellungspaket mithilfe des Assistenten Agent > **Agents bereitstellen**.
   - Das `KcsSetup`-Installationsprogramm überspringt die Installation, wenn es feststellt, dass sich bereits ein Agent auf einem Rechner befindet, falls der Schalter `/e` im Installationspaket vorliegt.
   - Sie werden wahrscheinlich die Option der automatischen Installation wählen.
   - Falls Benutzer, die das Anmeldeverfahren ausführen, keine Benutzerrechte haben, müssen gegebenenfalls Administrator-Anmeldedaten eingebunden werden.
2. Laden Sie über die Seite `dl.asp` das entsprechende `KcsSetup`-Installationspaket herunter und kopieren Sie es in eine Netzwerkfreigabe, von der aus Benutzer Programme ausführen können.
3. Fügen Sie die Datei `KcsSetup` mit ihrem Netzwerkpfad zum Anmeldeverfahren hinzu.

E-Mail

Senden Sie `KcsSetup` per E-Mail an alle Benutzer im Netzwerk. Laden Sie das entsprechende Installationspaket von der Seite **Agents bereitstellen** herunter und hängen Sie es an eine E-Mail auf Ihrem lokalen Rechner an. Sie können den Link des Standard-Installationspakets auch kopieren und in eine E-Mail-Nachricht einfügen. Fügen Sie Anleitungen zum Starten des Pakets ein, wie im nachstehenden Aufzählungspunkt **Manuell** beschrieben.

Ermittlung nach Netzwerk oder Domain

Verwenden Sie das **Discovery**-Modul, um Rechner in **Netzwerken** *(http://help.kaseya.com/webhelp/DE/KDIS/9000000/index.asp#1944.htm)* und **Domains** *(http://help.kaseya.com/webhelp/DE/KDIS/9000000/index.asp#10750.htm)* zu ermitteln. Installieren Sie dann die Agents manuell oder automatisch auf ermittelten Rechnern.

Automatische Kontenerstellung

Die *automatische Kontenerstellung muss* über System > **Check-in-Richtlinie** aktiviert werden, damit Sie automatisch ein Rechner-ID-Konto erstellen können, wenn ein Agent-Installationspaket installiert wird. Diese Option wird beim Installieren des VSA standardmäßig aktiviert.

Rechnergruppen neue Rechner-IDs nach IP-Adresse zuweisen

Sie können auch ein generisches Installationspaket erstellen, mit dem alle neuen Rechnerkonten zu der `unnamed` Gruppen-ID hinzugefügt werden. Wenn sich der Agent das erste Mal anmeldet wird ihm mit System > **Benennungsrichtlinie** die korrekte Gruppen-ID bzw. Untergruppen-ID unter Verwendung der IP-Adresse des verwalteten Rechners zugewiesen. Agent-Einstellungen können anschließend nach Richtlinie oder Vorlage konfiguriert werden. Siehe:

- **Konfigurieren von Agent-Einstellungen mit Richtlinien** *(siehe 25)*
- **Konfigurieren von Agent-Einstellungen mit Vorlagen** *(siehe 26)*

Agent-Installationspakete pflegen

Aktualisieren der Agent-Software

Ein Agent-Installationspaket lädt immer einen `KcsSetup.exe` herunter, der die neueste verfügbare Version der Agent-Software verwendet. Sobald die Datei `KcsSetup.exe` erstellt ist, bleibt ihre Version der Agent-Software innerhalb der exe-Datei fest. Erwägen Sie, `KcsSetup.exe`-Dateien zu ersetzen, die vor einer Weile erstellt und dann für eine einfache Verteilung in Netzwerkverzeichnissen gespeichert oder zu CDs hinzugefügt wurden. Auf gleiche Weise bleibt die auf dem Rechner installierte Version der Agent-Software immer fest, bis Sie sie über die Seite **Agent aktualisieren** *(siehe 61)* aktualisieren.

Standard-Installationspaket bearbeiten

Das `Default Install`-Paket stellt die Standardwerte ein, die beim Erstellen eines neuen Pakets angezeigt werden. Normalerweise kann das `Default Install`-Paket nicht geändert werden. Die Schaltfläche **Speichern** ist deaktiviert. Um die Schaltfläche **Speichern** für das `Default Install`-Paket zu aktivieren, führen Sie Folgendes *als Benutzer mit Master-Rolle* aus:

1. Klicken Sie in Agent > **Agents bereitstellen** auf die Schaltfläche **Gemeinsam nutzen** neben dem `Default Install`-Paket.
2. Aktivieren Sie **Anderen Benutzern Änderungen gestatten**.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie auf das Bearbeitungssymbol neben dem `Default Install`-Paket.

Wenn Sie das `Default Install`-Paket bearbeiten, ist die Schaltfläche **Speichern** aktiviert.

> **Hinweis:** Falls Sie das `Default Install`-Paket löschen, wird es sofort neu erstellt.

Agent-Einstellungen konfigurieren

Agent-Einstellungen

Agent-Einstellungen bestimmen das Verhalten des Agents auf dem verwalteten Rechner. Obgleich jeder Agent einzeln konfiguriert werden kann, wird das Verwalten von Rechnern vereinfacht, wenn Sie ähnliche Einstellungen für jeden Typ von verwaltetem Rechner festlegen. So können beispielsweise für Laptops, Desktops und Server Einstellungen festgelegt werden, die typisch für diesen Rechnertyp sind. Entsprechend können auch die Rechner eines Kunden eindeutige Merkmale aufweisen, die sich von denjenigen auf Rechnern anderer Kunden unterscheiden. Zu den Agent-Einstellungstypen zählen:

- **Anmeldedaten** *(siehe 56)*
- **Agent-Menü** *(siehe 45)*
- **Check-in-Kontrolle** *(siehe 48)*
- **Arbeitsverzeichnis** *(siehe 51)*
- **Protokolle** *(siehe 15)*
- **Profil bearbeiten** *(siehe 52)*
- Sammlungen ansehen
- **Portalzugriff** *(siehe 54)*
- Remote-Control-Richtlinie
- Patch-Einstellungen
- Patchdateiquelle
- Zugehörigkeit zu Patch-Richtlinien

- Meldungen
- Ereignisprotokoll-Meldungen
- Monitor-Sets
- Dateien verteilen
- Geplante Agent-Verfahren

Richtlinien im Vergleich zu Vorlagen

Es gibt zwei allgemeine Methoden für die Verwaltung von Agent-Einstellungen auf mehreren Rechnern.

- **Konfigurieren von Agent-Einstellungen mit Richtlinien** *(siehe 25)* – Dies ist die bevorzugte *dynamische* Methode für die Verwaltung von Agent-Einstellungen auf Hunderten, wenn nicht sogar Tausenden von Rechnern. Sobald eine Richtlinie auf einen Zielrechner angewendet wird, erfolgt die Übertragung automatisch.
- **Konfigurieren von Agent-Einstellungen mit Vorlagen** *(siehe 26)* – Dies ist die veraltete *statische* Methode für die Verwaltung von Agent-Einstellungen auf mehreren Rechnern. Agent-Einstellungen müssen bei jeder Änderung manuell auf die jeweiligen Zielrechner kopiert werden.

Konfigurieren von Agent-Einstellungen mit Richtlinien

Das **Policy Management**(KPM)-Modul im VSA verwaltet *Agent-Einstellungen nach Richtlinie*. Sobald den Rechnern, Rechnergruppen oder Organisationen Richtlinien zugewiesen wurden, *werden diese automatisch übertragen*, ohne dass der Benutzer weiter eingreifen muss.

Der Systemmanagement-Assistent

Es befindet sich ein Richtlinieninstallationsassistent auf der Registerkarte System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Systemmanagement.

Mit dem Einrichtungsassistenten können Sie schnell *Rechnerverwaltungsrichtlinien für eine bestimmte Organisation konfigurieren und anwenden.* Sind die Richtlinien konfiguriert, werden diese auf alle Rechner angewandt, die Sie im Auftrag der betreffenden Organisation verwalten. Richtlinien bestimmen viele verschiedene Aspekte der Rechnerverwaltung:

- Audit-Planung
- Monitoring
- Benachrichtigungen
- Patch-Verwaltung
- Rechner-Routinewartung mithilfe von Agentverfahren

Dank der Richtlinien müssen Sie nicht mehr jeden Rechner einzeln verwalten. Sie müssen nur eine Richtlinie zuweisen oder ändern. Eine Richtlinienzuweisung oder -änderung im Rahmen einer zugewiesenen Richtlinie wird innerhalb von 30 Minuten an alle beteiligten Rechner verteilt, ohne dass Sie in die Planung eingreifen müssen. Danach können Sie leicht feststellen, ob ein verwalteter Rechner die zugewiesenen Richtlinien erfüllt oder nicht. Die Verfolgung der Erfüllung jeder einzelnen Richtlinie liefert Ihnen die Informationen, die Sie für die zuverlässige Bereitstellung von IT-Diensten für die gesamte von Ihnen betreute Organisation benötigen.

> **Hinweis:** Eine detaillierte Erklärung jeder Option im **Installationsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/9000000/index.asp#11220.htm)* finden Sie im **Standard Solution Package**.

Konfigurieren von Agent-Einstellungen mit Vorlagen

Rechner-ID-Vorlagen

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > **Erstellen** *(siehe 34)*.
- Importieren Sie eine Rechner-ID-Vorlage über Agent **Import/Export** *(siehe 43)*.
- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > **Agents bereitstellen** *(siehe 19)*.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > **Einstellungen kopieren** *(siehe 42)*.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > Statistiken.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

So wenden Sie eine Rechner-ID-Vorlage auf ein Paket an:

1. Legen Sie mithilfe des **Paket erstellen**-Assistenten in **Agent bereitstellen** die Vorlage als die Quellrechner-ID fest, von der die Einstellungen kopiert werden sollen, wenn Sie das zu installierende Paket erstellen.
2. Fügen Sie mithilfe des gleichen Assistenten Attribute zu dem Paket hinzu. Diese zusätzlichen Attribute sind für gewöhnlich von Kunde zu Kunde verschieden und sollten daher nicht in der Vorlage gespeichert werden.

Agent-Einstellungen kopieren

Rechner-ID-Vorlagen werden anfänglich dazu verwendet, um ein Agent-Installationspaket zu erstellen. Dabei wird die Vorlage als Quelle verwendet, um Einstellungen zu kopieren. Aber selbst nach der Installation der Agents auf verwalteten Rechnern müssen Sie die Einstellungen auf vorhandenen Rechner-ID-Konten aktualisieren, da sich die Anforderungen Ihrer Kunden ändern und Sie sich immer besser mit dem VSA auskennen. Verwenden Sie in diesem Fall Agent > **Einstellungen kopieren**, um diese Änderungen auf alle Rechner-IDs zu kopieren, für die Sie Zugriffsberechtigungen haben. Achten Sie darauf, `Do Not Copy` für jede Einstellung auszuwählen, die Sie nicht überschreiben möchten. Verwenden Sie `Add`, um Einstellungen zu kopieren, ohne vorhandene Einstellungen zu entfernen. Kaseya empfiehlt, zuerst die Änderungen an einer ausgewählten Vorlage vorzunehmen und diese Vorlage dann als Quellrechner-ID zum Kopieren zu verwenden. Auf diese Weise wird sichergestellt, dass Ihre Rechner-ID-Vorlagen die "Master-Repositories" aller Ihrer Agent-Einstellungen bleiben und als Quelle für die Agent-Installationspakete und vorhandenen Rechner-ID-Konten dienen können.

Vorlagen und gefilterte Ansichten

Es besteht eine sinngemäße Beziehung zwischen den Rechner-ID-Vorlagen und dem Filtern Ihrer Ansicht von ausgewählten Rechnern mit der Ansichtdefinitionsoption **Nur ausgewählte Rechner-IDs anzeigen**. (Ansichtsdefinitionen werden in Arbeiten mit Agents im VSA) beschrieben.) Beim Definieren

einer Rechner-ID-Vorlage namens "Laptops" ist es beispielsweise einfacher, Einstellungen auf alle "Laptops" anzuwenden, für die Ihrer Verantwortung unterliegen, wenn Sie eine gefilterte Ansicht mit Namen "Laptops" besitzen. Wählen Sie ganz einfach die Ansicht für "Laptops" aus. Daraufhin werden auf jeder Funktionsseite nur Laptops angezeigt, egal zu welcher Rechnergruppe sie gehören. Entsprechendes gilt auch für "Desktops", "Workstations", Exchange-Server" usw.

Gefilterte Ansichten ausgewählter Rechner sind besonders dann nützlich, wenn Sie die Einstellungen von einer Rechner-ID-Vorlage mithilfe der oben beschriebenen Funktion **Einstellungen kopieren** auf bestehende Agents kopieren möchten.

Basis-Vorlagen und Inventarisierungen

Da Sie sich nie ganz sicher sein können, welche Einstellungen auf einen Rechner angewendet werden sollten, bis Sie eine Inventarisierung dieses Rechners durchführen, sollten Sie ein Agent-Paket installieren, das von einer "Basis"-Vorlage erstellt wurde, auf der die meisten Agent-Einstellungen *deaktiviert* sind. Sobald Sie die Inventarisierung durchgeführt haben, können Sie entscheiden, welche Einstellungen auf welchen Rechner angewendet werden sollen. Mit der Funktion **Einstellungen kopieren** können Sie Einstellungen von der entsprechenden Vorlage auf den neuen Agent kopieren.

Befehlszeilenschalter für Agent-Installation

In Befehlszeilenschaltern für Agent-Installationen für `KcsSetup` muss weder die Groß-/Kleinschreibung noch die Reihenfolge beachtet werden. Trennen Sie die Schalter durch eine Leerstelle. Zum Beispiel: `KcsSetup /e /g=root.unnamed /c`

> **Hinweis:** Bei Apple-Agents können Befehlszeilenschalter nur für die Erstellung des Agent-Installationspaketes verwenden werden.

`/b` – Das System wird nach Abschluss der Installation neu gestartet. Die Agent-Installation erfordert einen Neustart, damit die Treiber geladen werden können. Verwenden Sie diesen Schalter bei Paketen, die Benutzern gegeben wurden, die keine Rechte zum Abschalten des Rechners haben.

`/c` – Verwendet den Computernamen als Rechner-ID für das neue Konto. Falls der Computername nicht durch das Programm festgestellt werden kann, wird der Rechnerbenutzer zur Eingabe einer Rechner-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/d` – Verwendet den aktuellen Domänennamen als Gruppen-ID für das neue Konto. Falls der Domänenname nicht durch das Programm festgestellt werden kann, wird der Rechnerbenutzer zur Eingabe der Gruppen-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/e` – Die Installation wird sofort beendet, wenn das Installationsprogramm ermittelt, dass bereits ein Agent installiert ist. Verwenden Sie `/e` am Ende der Anmeldeverfahren. `/k` oder `/r` überschreibt `/e`.

`/f "Publisher"` – Gibt den vollen Namen des Dienstanbieters oder Tenant an. Nur Windows.

`/g=xxx` – Gibt die Gruppen-ID für das neue Konto an. `xxx` muss eine alphanumerische Zeichenfolge sein und darf keine Leerstellen oder Satzzeichen enthalten.

`/h` – Zeigt den Hilfedialog an, der alle Befehlszeilenschalter auflistet, es sei denn, der Schalter `/s` ist eingestellt. In diesem Fall wird die Anwendung beendet.

`/i` – Nicht kritische Fehler, z. B. falsche oder unbestimmte Versionen von WinSock2 oder unbestimmte Versionen des Betriebssystems werden ignoriert und das Fortsetzen der Installation wird erzwungen.

`/j` – Es wird kein Agent-Shortcut zum Menü **Start > Alle Programme** installiert. Nur Windows.

`/k` – Der Benutzer wird über ein Dialogfeld gefragt, ob eine Neuinstallation OK ist, wenn der Agent bereits auf dem Rechner ermittelt wurde. Ohne diesen Schalter wird das Installationsprogramm beendet, falls ein Agent bereits vorhanden ist.

`/m=xxx` – Gibt die Rechner-ID für das neue Konto an. `xxx` muss eine alphanumerische Zeichenfolge sein und darf keine Leerstellen oder Satzzeichen enthalten.

`/n = partitionId` – Gibt die Partition-ID der Tenant-Partition an, zu der das installierte Agent-/Rechner-ID-Konto gehört.

`/o "Company Title"` – Gibt den Firmentitel des Dienstanbieters oder Tenant an. Nur Windows.

`/p "install_path"` – Überschreibt den Standard-Installationspfad, indem der vollständige Verzeichnispfad (einschließlich des Laufwerksbuchstabens) angegeben wird, in dem der Agent installiert werden soll.

- Unter Windows erstellt die Agent-Installation standardmäßig ein Verzeichnis unter Verwendung des `%ProgramFiles%`-Variablenpfads als `\<company>\<Agent-Instance-Guid>`.
- Unter Linux erstellt die Agent-Installation standardmäßig ein Verzeichnis mit dem Namen `/opt/Kaseya/<Agent-Instance-Guid>`.
- Unter Apple wird der /p-Schalter nicht unterstützt und ignoriert.

> **Warnung:** Kaseya unterstützt die Installation von Agents im `%windir%` (normalerweise `c:\windows`)-Verzeichnis nicht.

`/r` – Führt das Installationsverzeichnis aus und installiert den Agent neu, selbst wenn bereits ein Agent auf dem Rechner vorhanden ist.

`/s` – Die Installation wird im automatischen Modus ausgeführt. Alle Dialogfelder werden unterdrückt.

`/t "Title"` – Gibt den Titel jedes Dialogfeldes an, das dem Benutzer während der Installation angezeigt wird. Der Standardtitel lautet: `"Kaseya Agent"`.

`/u` – Verwendet den aktuellen Rechnerbenutzernamen als Rechner-ID für das neue Konto. Falls der Rechnerbenutzername nicht durch das Programm festgestellt werden kann, wird der Benutzer zur Eingabe einer Rechner-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/v` – Ordnet diesen Agent einem bestehenden Agent-Konto im VSA zu, wenn Rechnername, Agent-Name und Organisation die gleichen für die gleiche Partition sind. Ignoriert das Erstellen eines neuen Agent-Kontos, wenn eine MAC-Adresse ermittelt wird. Geeignet für die Wiederverwendung von vorhandenen Agent-Konten, die für rückgängig gemachte VDI-Ressourcen erstellt wurden.

`/w` – Überschreibt die vorhandene Konfigurationsdatei mit einer in der Agent-Installation enthaltenen Konfigurationsdatei. Verwenden Sie dies mit dem Schalter `/r`, um einen Agent mit neuen Servereinstellungen zu installieren. Dies ist für einen bestehenden Agent beabsichtigt, der versucht, eine Verbindung mit einem nicht mehr existierenden Server herzustellen.

`/x` – Deaktiviert die Fernsteuerung, nachdem der Agent erfolgreich installiert wurde. Bei einer Aktualisierung oder Neuinstallation wird diese Option ignoriert. Die Fernsteuerung dieses Rechners kann erst erfolgen, wenn der Benutzer **Fernsteuerung aktivieren** auswählt, indem er mit der rechten Maustaste auf das K-Symbol in der Systemablage klickt.

`/z “Message”` – Gibt die Meldung an, die dem Benutzer nach Abschluss der Installation angezeigt wird. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation abgeschlossen und die Statusmeldung in das Installationsprotokoll geschrieben. Die Standardmeldung lautet: "`The Agent has been installed successfully on your computer.`"

`/?` – Zeigt den Hilfedialog an, der alle Befehlszeilenschalter auflistet, es sei denn, der Schalter `/s` ist eingestellt. In diesem Fall wird die Anwendung beendet. Nur Windows.

Installationsschalter nur für Linux

Siehe **Installation von Linux-Agents** *(siehe 31)*.

Probleme und Fehler bei der Installation

Beim Installieren von Agents können die folgenden Probleme und Fehlschläge eintreten:

- **Ungültige Anmeldedaten** – Die an das Paket gebundenen Anmeldedaten müssen über Administratorrechte auf dem lokalen Rechner verfügen. Der Agent wird als Systemdienst installiert und benötigt volle Benutzerberechtigungen, um erfolgreich installiert werden zu können. Der Administratorname kann ein Domänenbenutzer der Form `domain\administrator` oder `administrator@domain` sein. Stellen Sie bei Vista, 7 und 2008 Rechnern sicher, dass die Benutzerkontensteuerung (UAC) deaktiviert ist, damit Administrator-Anmeldedaten verwendet werden können.
- **Angegebene Domäne für einen Rechner ist nicht die Domäne** – Falls in Schritt 2 der Paketerstellung in **Agent bereitstellen** die Option **Domänenname** ausgewählt wird und der Computer nicht Teil einer Domäne ist, setzt ein Installationspaket den Prozessor bei 100 % fest. Es wird jedoch schließlich installiert.
- **Durch Anti-Virus-Programm blockiert** – Manche Anti-Virus-Programme können die Agent-Installation als Sicherheitsbedrohung klassifizieren und ihre Ausführung blockieren.
- **Durch Sicherheitsrichtlinie blockiert** – Lokale oder Domänen-Sicherheitsrichtlinien können den Zugriff auf das Installationsverzeichnis (normalerweise das Verzeichnis `Program Files`) verhindern.
- **Ungenügende Lizenzen** – Falls nicht genügend VSA-Lizenzen verfügbar sind, kann der Agent daran gehindert werden, sich zum ersten Mal anzumelden und ein Konto zu erstellen. Sollte dies geschehen, wird nach der Installation des Agents auf dem Rechner ein graues K-Symbol in der Systemablage angezeigt, das niemals zu blau wechselt. Wenn der Cursor auf das graue Agent-Symbol gesetzt wird, meldet ein angezeigter Tooltip "'Rechner-ID.Gruppen-ID' nicht vom Kaseya Server erkannt".

Apple

- Macintosh Agents können nicht ohne einen gültigen Benutzernamen und gültiges Kennwort bereitgestellt werden.

Mehrere Agents installieren

Es können mehrere Agents auf dem gleichen verwalteten Rechner installiert werden, wobei sich jeder bei verschiedenen Kaseya Servers anmeldet. *Führen Sie das v6-Agent-Installationsprogramm von einem anderen Kaseya Server* aus und Sie erhalten einen zusätzlichen Agent.

- Gilt für Windows- und Linux-Agents. Die Installation mehrerer Macintosh-Agents wird nicht unterstützt.
- Ein v6-Agent kann mit anderen v6-Agents koexistieren.
- Nur für Windows:
  - Ein v6-Agent kann mit v5.1- oder älteren Agents koexistieren.
  - Jeder verwaltete Rechner mit einem Domain-Controller-Anmeldeverfahren, auf dem das Agent-Installationsverfahren automatisch ausgeführt wird, *muss* die Datei `KcsSetup` aus der v5.1-Version oder einer älteren Version mit dem v6-Agent aktualisieren. Das v5.1- oder ältere Installationsprogramm erkennt den neueren v6-Agent nicht und wird neu installiert, selbst wenn der v6-Agent vorhanden ist.

Treibernutzung – nur Windows-Agents

Wenn mehrere Agents auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 62)*, **Netzwerkzugriff** *(siehe 64)* und **Anwendungsblocker** *(siehe 67)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese

Treiber kontrolliert.

- Die Treiber werden ursprünglich vom zuerst installierten Agent kontrolliert.
- Wenn der erste Agent, der die Treiber kontrolliert, deinstalliert wird, werden diese Treiber ebenfalls deinstalliert und diese drei Funktionen können von keinem Agent mehr ausgeführt werden.
- Diese Treiber werden durch eins der folgenden Ereignisse neu installiert:
  - Einer der vorhandenen Agents auf dem Rechner wird aktualisiert. Der aktualisierte Agent übernimmt die Kontrolle über die Treiber und kann diese drei Funktionen ausführen.
  - Ein neuer Agent wird installiert. Der neu installierte Agent übernimmt die Kontrolle über die Treiber und kann diese drei Funktionen ausführen.
- Informationen darüber, wie Sie ermitteln, welcher Agent die Kontrolle über die Treiber hat, finden Sie unter *Registrierung* weiter unten.

Agents auf verwalteten Rechnern identifizieren

Bei der Installation eines Kaseya-Agents wird ein *eindeutiger Identifikator* für ihn erstellt, der aus der 6-stelligen Kunden-ID des Kaseya Server und einer willkürlich erzeugten 14-stelligen Zahl besteht. Dieser eindeutige Identifikator wird als Agent-GUID bezeichnet. Er wird dazu verwendet, separate Unterordner zum Speichern von Agent-Programmdateien zu erstellen, und dient als Unterschlüssel für Agent-Registrierungswerte.

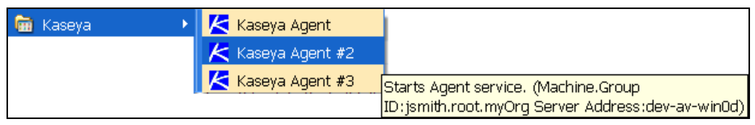
In den unten stehenden Beispielen zeigen Agents spezifische Informationen über die folgenden Platzhalter an:

- <GUID> – Die Agent-Instanz GUID.
- <company> – Das Installationsverzeichnis des Agents
- <serveraddress> – Die Kaseya Server-Adresse, bei der sich der Agent anmeldet.
- <machineID.groupID.orgID> – Die Rechner-ID, Gruppen-ID und Organisations-ID des Agents auf dem Kaseya Server.
- <shortcutname> – Der Name des Shortcut. Beispiel: Kaseya Agent #2.

Shortcuts

Wenn Sie den Mauszeiger über einem Shortcut für einen Kaseya-Agent bewegen, z. B. ein Shortcut im Windows-Startmenü, zeigt ein Tooltip Folgendes an:

- Start Agent service. (machine.GroupID:<machineID.groupID.orgID> Address:<serveraddress>)
- Wenn Sie mit der rechten Maustaste auf einen Shortcut klicken, wird dieser Text ebenfalls im Kommentarfeld der Shortcut-Eigenschaftsseite angezeigt.



Info zu Agent

Klicken Sie mit der rechten Maustaste auf das K-Symbol in der Systemablage eines verwalteten Rechners und wählen Sie die Option **Info zu Agent** aus, um die folgenden Informationen anzuzeigen:

- Agentversion
- Serveradresse – <serveraddress>
- Produkt-ID – <GUID>
- Programmtitel – <shortcutname>

Windows-Agents

Hinzufügen/Entfernen

Agents werden folgendermaßen angezeigt:

- `Kaseya Agent (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #2 (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #3 (<machineID.groupID.orgID> - <serveraddress>)`

Dienste

Im Beschreibungsfeld des Dienstes wird derselbe Text wie im oben stehenden Agent-Shortcut angezeigt.

Registry

Die Registrierungseinstellungen des Agents werden folgendermaßen angezeigt:

```
HKLM\Software\Kaseya\Agent
   DriverControl - The agent that controls driver usage.
   KES_Owned_By - The agent that manages the KES client.

HKLM\Software\Kaseya\Agent\<GUID>
   Title - <shortcutname>
   Path - C:\Program Files\<company>\<GUID>
   ServAddr - <serveraddress>
   machineID - <machineID.groupID.orgID>
   DriverControl - The agent that controls driver usage.
   KES_Owned - The agent that manages the KES client.
```

Standard-Agent-Installationsordner

- Siehe den `/p`-Schalter in **Befehlszeilenschalter für Agent-Installation** *(siehe 27)*.

Installation von Linux Agents

> **Hinweis:** Siehe **Systemvoraussetzungen** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm)* für Angaben zu unterstützten Linux-Betriebssystemen und Browsern.

Manuelle Installation von Linux Agents

1. Öffnen Sie einen Firefox oder Chrome Browser auf Ihrem Linux Rechner in einer Gnome-Sitzung und melden Sie sich am VSA an.
2. Zeigen Sie die Seite Agent > Agents installieren > **Agents verteilen** *(siehe 19)* an.
3. Klicken Sie auf den Hyperlink **Hier klicken um Standard-Agent herunterzuladen** und starten Sie den Download des Standard-Agent-Installationspaketes. Ein Linux Agent-Installationspaket wird heruntergeladen.

   > **Hinweis:** Alternativ können Sie Ihr eigenes Linux-Paket erstellen, indem Sie auf **Paket erstellen** drücken und sich durch den Installationsassistenten führen lassen.

4. Wenn der Download vollständig ist, suchen Sie die Datei `KcsSetup.sh` im Download-Verzeichnis des Linux Rechners.

> **Hinweis:** Wenn Sie `KcsSetup.exe` oder `KcsSetup.zip` heruntergeladen haben, haben Sie die falsche Installationsdatei heruntergeladen, weil das ausgewählte Installationspaket nur für Windows oder Macintosh gilt.

5. Führen Sie die folgenden Befehle als Stammverzeichnis aus:
```
# chmod +x KcsSetup.sh
# ./KcsSetup.sh
```
Der Agent wird installiert und startet. Melden Sie sich am VSA an und prüfen Sie den Agent-Status.

Weitere Informationen finden Sie in der Installationsprotokolldatei unter: `/tmp/KASetup_<pid>.log`
, wobei <pid> die Prozess-ID der `./KcsSetup.sh`-Ausführung ist.

> **Hinweis:** Führen Sie `KcsSetup.sh -V -D` für Verbose-Terminalausgabe aus.
>
> **Hinweis:** Führen Sie `KcsSetup.sh -X` aus, um die in der /tmp-Datei erstellten temporären Dateien auszuführen. Das Speichern dieser Dateien ist nützlich, wenn eine fehlgeschlagene Installation behoben wird.

6. Nachdem der Linux-Agent installiert ist, melden Sie sich an und wieder ab, damit Sie das Kaseya Agent-Symbol im Gnome-Panel sehen.

Installation von Linux Agents über LAN-Watch und Agents installieren

1. Planen Sie einen Discovery > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/9000000/index.asp#1944.htm)*-Scan und *nutzen Sie dafür einen bestehenden Linux-Agent als Ermittlungsrechner*.
2. Installieren Sie einen Linux-Agent auf einem ermittelten Linux-Rechner mit einer der Discovery > Ermittelte Geräte-Seiten.
   - Geben Sie `root` in das Feld **Admin-Anmeldung** ein.
   - Geben Sie das Kennwort für den `root`-Benutzer der anvisierten Linux Rechner im Feld **Kennwort** ein.
   - Wählen Sie ein Agent-Installationspaket aus dem Feld **Agent-Paket zur Installation wählen** aus.
   - Kreuzen Sie die Kontrollkästchen neben einem oder mehreren anvisierten Linux Rechnern an oder geben Sie die IP-Adresse oder den Namen des anvisierten Linux Rechner in das Feld **nicht gefundener Rechner** ein.
   - Klicken Sie auf die Schaltfläche **Abschicken**.

   > **Hinweis:** Die Seite **Agents installieren** unterscheidet aktuell nicht zwischen Linux und anderen Systemen. Die Person, die den Agent installiert, muss darauf achten, dass nur Linux Systeme ausgewählt werden.

Einen Linux Agent manuell deinstallieren

Ein `<install-dir>/bin/KcsUninstaller` wird immer mit dem Agent installiert und entfernt den Agent. Agents werden üblicherweise in das Verzeichnis `/opt` installiert.

Führen Sie die folgenden Befehle als Stammverzeichnis aus:
```
# ./KcsUninstaller
```

> **Hinweis:** Führen Sie den Befehl `./KcsUninstaller -D -V` aus, um den Agent mit Verbose-Terminalausgabe zu deinstallieren.

Fehlerbehebung bei Linux-Agent-Installationen

- Siehe die Community-Seite **Fehlerbehebung bei Linux-Agent-Installationen** *(https://helpdesk.kaseya.com/entries/36223968)*.

Unterstützte Linux Funktionen

Linux Agents unterstützen die folgenden Funktionen:

- Agent-Verfahren
- Letzte Audits, Basis-Audits und System-Audits
- Remote Control und FTP mit VNC
- SSH
- Kennwort zurücksetzen
- LAN-Watch und Agents installieren – Siehe **Linux Agents installieren** *(siehe 31)*.
- Meldungen
- Überwachung der Prozesse
- Überwachung von SNMP
- Log-Parser
- Benutzerspezifische Site-Anpassung – Die Registerkarte **Agent-Symbole** bietet jetzt einen Symbolsatz für Linux Agents, die Sie anpassen können.
- Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Dazu gehören:
- Live-Connect – Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Unterstützte Menüoptionen wie folgt:
  - Startseite
  - Agent-Daten
  - Audit-Information
  - Ticketing (oder Service-Desk-Ticketing)
  - Chat
  - Video-Chat

Siehe **Systemanforderungen** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm)*.

Unterstützte Apple-Funktionen

Apple-Agents unterstützen die folgenden Funktionen:

- Audits – Ausgewählte Hardware- und Software-Attribute
- Agent-Verfahren
- Remote Control
- FTP
- SSH
- Kennwort zurücksetzen
- Task-Manager
- Live-Connect mit Desktopzugriff.
  - Auf Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, können Sie Desktopzugriff in Live-Connect nutzen, um ein Windows System, das Firefox oder Safari verwendet, remote zu steuern.

  - Unter Verwendung einer unserer unterstützten Browser können Sie unter Windows Desktop-Zugriff verwenden, um Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, remote zu steuern.
- LAN-Watch über Ermittlung
- Monitoring wurde unterstützt:
  - SNMP-Monitoring
  - Monitoring in Monitor-Sets verarbeiten
  - Systemprüfung
  - Log-Parser

Siehe **Systemanforderungen** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm)*.

Erstellen

Agent > Agents installieren > Erstellen

Auf der Seite **Erstellen** werden ein Rechner-ID-Konto und Agent-Installationspaket für einen *einzigen* Rechner erstellt. Sie erstellen zuerst das Rechner-ID-Konto und dann ein Installationspaket für den Rechner. Normalerweise gilt die Seite **Erstellen** für Folgendes:

- **Rechner-ID-Vorlagen** – In diesem Fall braucht kein Installationspaket erstellt zu werden, da Rechner-ID-Vorlagen nicht zur Installation auf einem Rechner gedacht sind.
- **Neuinstallieren von Agents für ein vorhandenes Konto** – Da die Installationspakete **Erstellen** *nicht automatisch ein neues Rechner-ID-Konto erstellen*, können Sie die Seite **Erstellen** verwenden, um Agents auf verwalteten Rechnern für *vorhandene* Konten *neu zu installieren*.
- **Gesicherte Umgebungen** – Gesicherte Umgebungen erfordern eventuell eine manuelle Einrichtung jedes Rechners. Vielleicht müssen Sie beispielsweise ein neues Rechner-ID-Konto manuell benennen und/oder ein Agent-Installationspaket mit eindeutigen Anmeldedaten für einen einzelnen Rechner erstellen. Ein Benutzer muss lokal bei einem Zielrechner angemeldet sein, um das Paket zu installieren.

Hinweis: Verwenden Sie Agent > **Agents erstellen** *(siehe 19)*, um Agent-Installationspakete zu erstellen und auf *verschiedenen* Rechnern zu installieren. Das Installationspaket **Agents bereitstellen** *erstellt automatisch ein Rechner-ID-Konto*, wenn es installiert wird. Dazu muss jedoch die automatische Kontenerstellung über System > Check-in Policy aktiviert worden sein.

Hinweis: Verwenden Sie **Discovery**, um Agents auf *Remote-Systemen* zu installieren.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der Rechner-ID/Gruppen-ID/Organisations-ID und dem Agent zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Agent-Lizenzzahlen

Die folgenden Ereignisse wirken sich auf Agent-Lizenzzahlen aus:

- Eine "nicht verwendete" Agent-Lizenz wird in "verwendet" geändert, wenn ein Rechner-ID-Konto erstellt und der Agent installiert wird.
- Falls der Agent, aber nicht das Konto, gelöscht wird, wird die Agent-Lizenz dennoch als "verwendet" betrachtet.

- Wenn das Konto gelöscht wird (ungeachtet dessen, was mit dem Agent geschieht), erhält die Agent-Lizenz wieder den Status "nicht verwendet".
- Falls ein Konto erstellt wird, der Agent jedoch noch nicht zum ersten Mal installiert ist, wird das Konto als Rechner-ID-Vorlage bezeichnet. Rechner-ID-Kontovorlagen werden erst als "verwendet" gezählt, wenn Sie den Agent installieren.

Anmeldedaten in Agent-Installationspakete einschließen

Gegebenenfalls kann ein Agent-Installationspaket erstellt werden, das Anmeldedaten eines Administrators für den Zugriff auf ein Kundennetzwerk enthält. Anmeldedaten sind nur erforderlich, wenn Benutzer Pakete auf Rechnern installieren und *keinen Administratorzugriff* auf ihr Netzwerk haben. Die Anmeldedaten des Administrators sind verschlüsselt, niemals als Klartext verfügbar und an das Installationspaket gebunden.

Auswahl des Betriebssystems

Agent-Pakete können erstellt werden, um Agents auf Rechnern zu installieren, auf denen Windows-, Apple- oder Linux-Betriebssysteme laufen. Es kann jedoch auch automatisch das Betriebssystem des Rechners, der den Agent herunterlädt, gewählt werden.

Rechner-ID-Vorlagen

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > **Erstellen** *(siehe 34)*.
- Importieren Sie eine Rechner-ID-Vorlage über Agent **Import/Export** *(siehe 43)*.
- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > **Agents bereitstellen** *(siehe 19)*.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > **Einstellungen kopieren** *(siehe 42)*.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > Statistiken.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

Vordefinierte Meldungen

Wenn Sie über Agent > **Erstellen** ein Rechner-ID-Konto erstellen *und Einstellungen nicht von einem anderen Rechner kopieren*, werden verschiedene typische Benachrichtungen für das Rechner-ID-Konto standardmäßig erstellt.

Neue Konten-Einstellungen kopieren aus

Klicken Sie auf ein Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID. Agent-Einstellungen werden von dieser Rechner-ID kopiert.

> **Hinweis:** Wenn Sie keine Rechner-ID angeben, von der kopiert werden soll, und auf **Erstellen** klicken, wird ein neues, verwendbares Rechner-ID-Konto mit den Kaseya Server-Standardwerten erstellt.

Neue Rechner-ID

Geben Sie einen eindeutigen Namen für die neue Rechner-ID ein, die Sie erstellen.

Gruppen-ID

Wählen Sie eine vorhandene Gruppen-ID für die neue Rechner-ID aus, die Sie erstellen. Der Standard ist `root.unnamed`. Gruppen-IDs werden von einem VSA-Benutzer über System > Org. / Gruppen / Abtlg.> Verwalten erstellt.

Erstellen

Klicken Sie auf **Erstellen**, um die neue Rechner-ID für die ausgewählte Gruppen-ID zu erstellen.

Neue Konten einrichten/löschen, die in Gruppen-ID <Gruppen-ID>, Einstellungen kopieren von <Rechner-ID> erstellt wurden

Sie können für jede Gruppen-ID eine andere Standard-Rechner-ID angeben, von der die Einstellungen kopiert werden sollen.

1. Wählen Sie eine Rechner-ID aus, von der Einstellungen kopiert werden sollen, indem Sie auf das Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID klicken.
2. Wählen Sie eine Gruppen-ID aus der Dropdown-Liste mit den Gruppen-IDs aus.
3. Klicken Sie auf **Einrichten**, um sicherzustellen, dass die neue, für die ausgewählte Gruppen-ID erstellte Rechner-ID die Einstellungen von der ausgewählten Standard-Rechner-ID kopiert.
4. Klicken Sie auf den Link **Löschen**, um diese Zuweisung zu entfernen.

Konten einrichten/löschen, die in *nicht zugewiesenen* Gruppen-ID-Kopiereinstellungen von <Rechner-ID> erstellt wurden

Diese Option gibt die Standard-Rechner-ID an, von der Einstellungen kopiert werden sollen, falls keine Standard-Rechner-ID für eine Gruppen-ID eingestellt wurde. Diese Option wird nur für Masterrollenbenutzer angezeigt.

1. Wählen Sie eine Rechner-ID aus, von der Einstellungen kopiert werden sollen, indem Sie auf das Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID klicken. Anfangs ist dieser Wert auf *nicht zugewiesen* eingestellt.
2. Klicken Sie auf **Einrichten**, um sicherzustellen, dass neue, ohne Gruppen-Standard-Rechner-ID erstellte Rechner-IDs die Einstellung von der Standard-Rechner-ID des Benutzers mit Master-Rolle kopieren. Anfänglich ist dieser Wert auf *nicht zugewiesen* eingestellt.
3. Klicken Sie auf den Link **Löschen**, um diese Zuweisung zu entfernen.

Kontaktinformationen eingeben

Wenn Sie auf dieser Seite Kontaktinformationen für ein neues Rechner-ID-Konto eingeben und dieses neue Konto dann durch Klicken auf die Schaltfläche **Erstellen** anlegen, werden dieselben Kontaktinformationen auf die Seite Agent > **Profil bearbeiten** *(siehe 52)* übertragen. Die Kontaktinformationen umfassen Folgendes:

- **Kontakt-E-Mail** – Geben Sie die E-Mail-Adresse der Person ein, die den verwalteten Rechner benutzt.
- **Auto** – Aktivieren Sie **Auto**, um das Feld **Kontakt-E-Mail** automatisch mit einer E-Mail-Adresse im folgenden Format auszufüllen: `machineid@groupid.com`. Diese Funktion setzt voraus, dass Sie Rechner-IDs und Gruppen-IDs erstellen, die sich an die E-Mail-Adressen der Benutzer anpassen.
- **Kontaktname** – Geben Sie den Namen der Person ein, die den verwalteten Rechner benutzt.

- **Kontakt Telefon** – Geben Sie die Telefonnummer der Person ein, die den verwalteten Rechner benutzt.
- **E-Mail Administrator** – Geben Sie die E-Mail-Adresse der Person ein, die für den IT-Support für den verwalteten Rechner zuständig ist.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Einstellungen kopieren

Klicken Sie auf ein Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID. Die Einstellungen der Rechner-ID werden von dieser Rechner-ID kopiert.

Agent-Installation herunterladen/per E-Mail versenden

Klicken Sie auf einen Link für eine Rechner-ID, um mithilfe des Assistenten **Agent herunterladen** ein Installationspaket für ein vorhandenes Rechner-ID-Konto zu erstellen und zu verteilen.

Hinweis: Ein mit dieser Seite erstelltes Installationspaket gilt für spezifische Rechner-ID-Konten. Verwenden Sie **Agent verteilen** *(siehe 19)*, um Installationspakete für *mehrere* Rechner zu erstellen.

1. Wählen Sie das Betriebssystem aus, für das Sie das Installationspaket erstellen: `Windows`, `Macintosh` oder `Linux`.
2. Binden Sie optional die Anmeldedaten eines Benutzers an das Installationspaket. Füllen Sie das Formular mit den Administratoranmeldedaten aus, um die Benutzerrechte sicher an das Installationsformular zu binden.
   - Benutzer ohne Benutzerrechte können das Installationspaket erfolgreich installieren, ohne Administrator-Anmeldedaten eingeben zu müssen.
   - Wenn die Administrator-Anmeldedaten leer gelassen werden und der Benutzer keine Rechte zum Installieren von Software hat, wird er während der Installation vom Installationspaket zur Eingabe von Administrator-Anmeldedaten aufgefordert.
3. Wählen Sie die Verteilungsmethode aus.
   - **Herunterladen** – Laden Sie das Installationspaket sofort auf den gegenwärtig von Ihnen benutzten Rechner herunter. Der Name des Installationspakets lautet stets `KcsSetup`.
   - **E-Mail** – Senden Sie eine Textnachricht per E-Mail, die einen Link zum Herunterladen des Installationspakets enthält.

Typ

Dies ist der Typ des auf dem verwalteten Rechner verwendeten Betriebssystems:

- Fenster
- Macintosh
- Linux

Erstes Check-in

Listet die Uhrzeit auf, zu der jeder Agent sich zum ersten Mal am Kaseya Server angemeldet hat.

Löschen

Agent > Agents installieren > Löschen

Auf der Seite **Löschen** können drei verschiedene Kombinationen von *Rechner-ID-Konten* und *Agents* gelöscht werden.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der Rechner-ID/Gruppen-ID/Organisations-ID und dem Agent zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Agent-Lizenzzahlen

Die folgenden Ereignisse wirken sich auf Agent-Lizenzzahlen aus:

- Eine "nicht verwendete" Agent-Lizenz wird in "verwendet" geändert, wenn ein Rechner-ID-Konto erstellt und der Agent installiert wird.
- Falls der Agent, aber nicht das Konto, gelöscht wird, wird die Agent-Lizenz dennoch als "verwendet" betrachtet.
- Wenn das Konto gelöscht wird (ungeachtet dessen, was mit dem Agent geschieht), erhält die Agent-Lizenz wieder den Status "nicht verwendet".
- Falls ein Konto erstellt wird, der Agent jedoch noch nicht zum ersten Mal installiert ist, wird das Konto als Rechner-ID-Vorlage bezeichnet. Rechner-ID-Kontovorlagen werden erst als "verwendet" gezählt, wenn Sie den Agent installieren.

Löschen von Agents mit Tickets

Durch Löschen eines Rechnerkontos werden alle **Service Desk**-Tickets oder **Ticketing**-Tickets der Rechnergruppe oder Organisation, zu der das Rechnerkonto gehört hat, erneut zugeordnet.

Verfahren

1. Wählen Sie im Seitenbereich eine oder mehrere Rechner-IDs aus.
2. Klicken Sie auf eins der folgenden Optionsfelder:
   - **Agents erst bei der nächsten Anmeldung deinstallieren** – Deinstallieren Sie den Agent vom Rechner **und** entfernen Sie das Rechner-ID-Konto vom Kaseya Server. Das Konto wird erst bei der nächsten erfolgreichen Anmeldung des Agents gelöscht.
   - **Konto jetzt löschen, ohne den Agent zu deinstallieren** – Der Agent bleibt installiert **und** das Rechner-ID-Konto wird vom Kaseya Server entfernt.
   - **Agent deinstallieren und Konto beibehalten** – Deinstallieren Sie den Agent vom Rechner, **ohne** das Rechner-ID-Konto vom Kaseya Server zu entfernen.
3. Klicken Sie auf die Schaltfläche **Konten löschen**.

> **Hinweis:** Durch die Deinstallation eines Agents wird K-VNC oder der KBU-Client, KES-Client oder KDPM-Client nicht entfernt. Vor dem Löschen des Agents verwenden Sie Fernsteuerung > Fernsteuerung deinstallieren, um K-VNC auf den verwalteten Rechnern zu deinstallieren. Deinstallieren Sie ebenfalls alle Clients des Zusatzmoduls.

Wählen Sie alte Konten aus, die seit<Datum> nicht mehr angemeldet waren.

Klicken Sie auf den Hyperlink **Alte auswählen**, um alle Rechner-IDs im Seitenbereich zu markieren, die seit dem angegebenen Datum nicht mehr angemeldet waren. Dies stellt eine einfache Methode zum Identifizieren und Entfernen veralteter Rechner-IDs dar.

Datenbank bereinigen

Das Entfernen eines Rechner-Kontos über diese Seite **Löschen** markiert das Rechnerkonto für den Löschvorgang. Der tatsächliche Löschvorgang findet normalerweise außerhalb der Arbeitsstunden statt, um die Ressourcen während des Arbeitstages zu schonen. In einigen Fällen ist es nützlich, Rechnerkonten sofort zu bereinigen. Beispielsweise könnte der Kaseya Server die Agent-Lizenzzahl überschreiten. Klicken Sie auf **Datenbank bereinigen**, um Rechnerkonten sofort zu löschen, die bereits für den Löschvorgang markiert wurden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Letzter Check-in

Zeigt die Uhrzeit an, zu der der Rechner-Agent zum letzten Mal am Kaseya Server angemeldet waren. Bei Agents, die länger nicht angemeldet waren, werden diese Informationen als roter Text angezeigt.

Umbenennen

Agent > Agents installieren > Umbenennen

Auf der Seite **Umbenennen** werden vorhandene Rechner-ID-Konten umbenannt. Sie können die Rechner-ID ändern und/oder einer anderen Gruppen-ID zuweisen.

Agents werden durch eine eindeutige GUID-Nummer identifiziert. Durch ein Umbenennen des Agents wird nur der Anzeigename des Agenta geändert, und zwar sowohl auf dem Kaseya Server als auch in der Option **Konto festlegen...** im Agent-Menü des verwalteten Rechners.

> **Hinweis:**Informationen über das Zuweisen mehrerer Rechner zu einer anderen Gruppen-ID finden Sie unter Agent > **Gruppe ändern** *(siehe 41)*.

Verfahren

1. Wählen Sie im Seitenbereich eine Rechner-ID aus.
2. Klicken Sie auf eins der folgenden Optionsfelder:
   - **Konto umbenennen** – Wählen Sie diese Option aus, um ein ausgewähltes Rechner-ID-Konto umzubenennen.
   - **Offline Konto zusammenführen <Offline Rechner-ID> in <Rechner-ID auswählen> <Offline Rechner-ID>nach Zusammenführung** löschen – Verwenden Sie die Zusammenführung, um Protokolldaten von zwei verschiedenen Konten auf demselben Rechner zu kombinieren. Dies könnte notwendig sein, wenn ein Agent deinstalliert und dann unter einem anderen Kontonamen neu installiert wurde. Bei einer Zusammenführung werden die Konten wie folgt kombiniert:
     - ✓ Protokolldaten von beiden Konten werden kombiniert.
     - ✓ Daten des Basis-Audits vom alten Offline Konto ersetzen alle Ausgangsdaten im ausgewählten Konto.
     - ✓ Meldungseinstellungen vom ausgewählten Konto bleiben erhalten.
     - ✓ Anstehende Agent-Verfahren vom ausgewählten Konto bleiben erhalten. Anstehende Agent-Verfahren vom alten Offline-Konto werden verworfen.
     - ✓ Das alte Konto wird nach der Zusammenführung gelöscht.

     Hinweis: Da der Rechner nur auf einem einzigen Konto aktiv sein kann, werden nur Offline-Konten zur Zusammenführung in der Dropdown-Liste angezeigt.
3. Geben Sie optional einen **Neuen Namen** für das Rechner-ID-Konto ein.
4. Wählen Sie optional eine andere **Gruppen-ID** für das Rechner-ID-Konto aus.
5. Klicken Sie auf die Schaltfläche **Umbenennen**.

Umbenennen

Klicken Sie auf **Umbenennen**, um den Namen eines ausgewählten Rechner-ID-Kontos mithilfe der früher ausgewählten Optionen zu ändern.

Neuer Name

Geben Sie den **Neuen Namen** für die ausgewählte Rechner-ID ein.

Gruppen-ID

Wählen Sie die **Gruppen-ID** aus, die dem ausgewählten Rechner-ID-Konto zugewiesen werden soll. Bei Wahl des Standardwerts bleibt die Gruppen-ID unverändert.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen. Klicken Sie auf das Optionsfeld links von dem Rechnerkonto, das Sie umbenennen möchten.

Neuer Name beim nächsten Check-in

Listet den neuen Namen auf, auf den das Konto bei der nächsten Anmeldung des Agents umbenannt wird. Hier werden nur anstehende Umbenennungen angezeigt.

Gruppe ändern

Agent > Agents installieren > Gruppe ändern

Auf der Seite **Gruppe ändern** werden mehrere Rechner-IDs zu verschiedenen Gruppen-IDs zugewiesen. Rechner, die gegenwärtig offline sind, werden bei ihrem nächsten Check-in zugewiesen.

Rechner-ID in eine andere Gruppe verschieben

1. Wählen Sie im Seitenbereich eine oder mehrere Rechner-IDs aus.
2. Wählen Sie eine Gruppen-ID aus dem Dropdown-Menü **Neue Gruppen-ID auswählen** aus.
3. Klicken Sie auf die Schaltfläche **Verschieben**.

Verschieben

Weist ausgewählte Rechner-IDs zur ausgewählten Gruppen-ID zu.

Neue Gruppen-ID auswählen

Geben Sie die neue Gruppen-ID an, die jeder ausgewählten Rechner-ID zugewiesen werden soll.

> **Hinweis:** Erstellen Sie über System > Benutzersicherheit > Scopes eine neue Rechnergruppen-ID oder Untergruppen-ID.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter**

(siehe 5) und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Einstellungen kopieren

Agent > Agent konfigurieren > Einstellungen kopieren

Auf der Seite **Einstellungen kopieren** können Sie ausgewählte Einstellungen von einer einzigen Quellrechner-ID auf mehrere Rechner-IDs kopieren. Sie können Einstellungen jeweils *von nur einer Quell*rechner-ID oder -Vorlage kopieren. Aber Sie können verschiedene Einstellungstypen von verschiedenen Quellrechner-IDs oder -Vorlagen in Folge kopieren.

Einstellungen und Vorlagen kopieren

Rechner-ID-Vorlagen werden anfänglich dazu verwendet, um ein Agent-Installationspaket zu erstellen. Dabei wird die Vorlage als Quelle verwendet, um Einstellungen zu kopieren. Aber selbst nach der Installation der Agents auf verwalteten Rechnern müssen Sie die Einstellungen auf vorhandenen Rechner-ID-Konten aktualisieren, da sich die Anforderungen Ihrer Kunden ändern und Sie sich immer besser mit dem VSA auskennen. Verwenden Sie in diesem Fall Agent > **Einstellungen kopieren**, um diese Änderungen auf alle Rechner-IDs zu kopieren, für die Sie Zugriffsberechtigungen haben. Achten Sie darauf, `Do Not Copy` für jede Einstellung auszuwählen, die Sie nicht überschreiben möchten. Verwenden Sie `Add`, um Einstellungen zu kopieren, ohne vorhandene Einstellungen zu entfernen. Kaseya empfiehlt, zuerst die Änderungen an einer ausgewählten Vorlage vorzunehmen und diese Vorlage dann als Quellrechner-ID zum Kopieren zu verwenden. Auf diese Weise wird sichergestellt, dass Ihre Rechner-ID-Vorlagen die "Master-Repositories" aller Ihrer Agent-Einstellungen bleiben und als Quelle für die Agent-Installationspakete und vorhandenen Rechner-ID-Konten dienen können.

Kopie

Klicken Sie auf **Kopieren**, um einen Quellrechner auszuwählen. Nach Auswahl des Quellrechners werden die Einstellungstypen, die Sie kopieren können, in einem zweiten Fenster angezeigt.

Indem Sie nur bestimmte Typen von Einstellungen zum Kopieren auswählen, können Sie verhindern, dass kundenspezifische Einstellungen überschrieben werden, die Sie beibehalten möchten. Dazu zählt z. B. die `Patch File Source`, die für jeden Kunden unterschiedlich ist.

Wählen Sie die Option `Add` aus, um Einstellungen zu Zielrechnern hinzuzufügen, ohne vorhandene Einstellungen zu ersetzen.

Es können folgende Typen von Agent-Einstellungen kopiert werden:

- Anmeldedaten
- Agent-Menü
- Check-in-Kontrolle
- Arbeitsverzeichnis
- Protokolle
- Rechnerprofil – Verweist auf Einstellungen in Inventarisierung > **Profil bearbeiten** *(siehe 52)*.
- Sammlungen ansehen
- Portalzugriff
- Remote-Control-Richtlinie
- Patch-Einstellungen
- Patchdateiquelle
- Zugehörigkeit zu Patch-Richtlinien
- Feste Meldungen – Diese Meldungstypen werden alle auf der Seite Monitor > Meldungen angezeigt, mit Ausnahme von `Event Log`-Meldungen und `System`-Meldungen.
- Ereignisprotokoll-Meldungen

- Monitor-Sets
- Dateien verteilen
- Schutz
- Geplante Skripte

Wählen Sie die Rechner-ID aus

Klicken Sie auf den Link **Rechner-ID auswählen**, um anzugeben, von welcher Rechner-ID die Einstellungen kopiert werden sollen.

Verteilen Sie die geplanten Skripte auf unterschiedliche Zeiten, wenn Sie sie auf mehrere Rechner kopieren

Sie können die Last auf das Netzwerk verteilen, indem Sie diese Aufgabe staffeln. Wenn Sie diesen Parameter auf 5 Minuten einstellen, wird der Scan auf jeder Rechner-ID um 5 Minuten versetzt. Beispiel: Rechner 1 läuft um 10:00, Rechner 2 läuft um 10:05, Rechner 3 läuft um 10:10.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits
Agent online
Agent online und Benutzer gegenwärtig angemeldet.
Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
Agent ist gegenwärtig offline
Agent hat nie eingecheckt.
Agent ist online, aber die Fernsteuerung wurde deaktiviert.
Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Status

Zeigt den Rechnernamen, von dem die Einstellungen kopiert wurden und die Uhrzeit des Kopiervorgangs.

Import/Export

Agent > Agent konfigurieren > Import/Export

Auf der Seite **Import/Export** können Einstellungen für Rechner-ID-Konten als XML-Dateien importiert und exportiert werden, einschließlich geplanter Agent-Verfahren, zugewiesener Monitor-Sets und Ereignissätze. Protokolldaten sind nicht im Import oder Export eingeschlossen. Mit **Import/Export** können Sie Einstellungen für Rechner-ID-Konten, darunter Rechner-ID-Vorlagen, von einem Kaseya Server zum nächsten migrieren.

- Stellen Sie beim Importieren einer XML-Datei sicher, dass die Verschlüsselung der Datei ISO-8859-1 lautet.
- Eine Liste der mit einem Rechner-ID-Konto verknüpften Einstellungstypen finden Sie unter **Einstellungen kopieren** *(siehe 42)*.
- Die neuesten Anweisungen zur Migration eines vorhandenen Kaseya Server auf einen neuen Rechner finden Sie im Abschnitt *Verschieben des Kaseya Server* in den aktuellen **Kaseya Server-Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/Install/index.asp#home.htm)*.
- Beispielvorlagen für bestimmte Rechnertypen können Sie von unserer Website aus dem Kaseya Forum **Kaseya Connections** unter **http://community.kaseya.com** *(http://community.kaseya.com)* kopieren.

So exportieren Sie Rechner-ID-Einstellungen:

1. Klicken Sie auf den Link **Rechner auswählen**. Es wird ein Dialogfeld zur Auswahl des Rechners angezeigt.
2. Filtern Sie optional die Anzeige der aufgelisteten Rechner-IDs unter Verwendung des Rechner-ID/Gruppen-ID-Filters.
3. Klicken Sie auf einen Rechner-ID-Link für den Export. Die ausgewählte Rechner-ID wird nun auf der Seite **Import/Export** angezeigt.
4. Klicken Sie auf **Export**. Die Seite zeigt einen XML-Auszug der exportierten Agent-Einstellungen an.
5. Exportieren Sie die XML-Anweisung wie folgt:
   - Kopieren Sie den XML-Text in die Zwischenablage.
   - Klicken Sie mit der rechten Maustaste auf den Link **Herunterladen** und wählen Sie die Option **Ziel speichern unter**, um den XML-Text als XML-Datei auf Ihrem lokalen Computer zu speichern.

So importieren Sie Rechner-ID-Einstellungen:

1. Stellen Sie beim Importieren einer XML-Datei sicher, dass die Verschlüsselung der Datei ISO-8859-1 lautet.
2. Klicken Sie auf **Blättern**, um eine XML-Datei auszuwählen, die die Einstellungen eines Rechner-ID-Kontos darstellt. Normalerweise werden diese XML-Dateien durch den Export von einem anderen Kaseya Server erstellt.
3. Klicken Sie auf **Import**. Es wird ein Satz zusätzlicher Optionen angezeigt.
4. Akzeptieren Sie den Namen der Rechner-ID oder geben Sie einen an. Wenn dieser Name noch nicht auf dem Kaseya Server vorhanden ist, wird ein neuer Name erstellt.
5. Akzeptieren Sie oder wählen Sie eine andere Gruppen-ID aus.
6. Aktivieren Sie optional das Kontrollkästchen neben **Bestehende Daten ersetzen, falls diese Rechner-ID bereits existiert**.
7. Ändern Sie optional die E-Mail-Benachrichtigungsadresse für alle Meldungen, die für dieses Rechner-ID-Konto definiert sind.
8. Klicken Sie auf **Fertig stellen**, um den Import abzuschließen.

Aussetzen

Agent > Agent konfigurieren > Aussetzen

Auf der Seite **Aussetzen** werden alle Agent-Operationen, z. B. Agent-Verfahren, Monitoring und Patching ausgesetzt, ohne die Einstellungen des Agents zu ändern. Wenn eine Aktion ausgesetzt wird, erscheint neben der Rechner-ID wird das Symbol Aussetzen . Wenn ein Rechner-ID-Konto

ausgesetzt ist, wird auf dem verwalteten Rechner ein graues Agent-Symbol in der Systemablageangezeigt.

Mit der Option **Rechner zeigen, die ausgesetzt/nicht ausgesetzt sind** in **Ansichtdefinitionen** *(siehe 6)* können Sie die Anzeige der Rechner-IDs auf jeder Agent-Seite filtern.

Aussetzen

Klicken Sie auf **Aussetzen**, um Agent-Operationen auf ausgewählten Rechner-IDs auszusetzen.

Fortsetzen

Klicken Sie auf **Fortsetzen**, um Agent-Operationen auf ausgewählten Rechner-IDs fortzusetzen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Ausgesetzt

Zeigt `Suspended` an, wenn die Rechner-ID ausgesetzt ist.

Agent-Menü

Agent > Agent konfigurieren > Agent-Menü

Auf der Seite **Agent-Menü** werden die Optionen festgelegt, die im Agent-Menü des Rechners eines Benutzers angezeigt werden. Der Benutzer zeigt das Agent-Menü an, indem er mit der rechten Maustaste auf das Agent-Symbol in der Systemablagedes verwalteten Rechners klickt. Über diese Seite kann außerdem *verhindert werden*, dass das Agent-Symbol auf dem Rechner des Benutzers angezeigt wird. Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.

> **Hinweis:** Eine allgemeine Erläuterung der Anzeige von Agent-Symbolen auf dem Rechner des Benutzers finden Sie unter **Agent-Symbole** *(siehe 3)*.

Agent-Symbol auf dem Rechner des Benutzers ausblenden

So blenden Sie das Agent-Symbol vollkommen aus:

1. Wählen Sie eine oder mehrere Rechner-IDs aus.
2. Deaktivieren Sie das Kontrollkästchen **Agent-Symbol aktivieren**.
3. Klicken Sie auf **Aktualisieren**.

Alle anderen Kontrollkästchen-Einstellungen werden abgeblendet angezeigt. Dies bedeutet, dass alle Optionen des Agent-Menüs deaktiviert wurden.

Benutzer daran hindern, den Agent-Dienst auf dem Rechner zu beenden

Falls die Option **Beenden** auf dem verwalteten Rechner eines Benutzers aktiviert ist, kann er den Agent-Dienst auf dem Rechner durch Auswahl dieser Option beenden. Wenn der Agent-Dienst angehalten wird, wird der verwaltete Rechner für VSA-Benutzer als offline angezeigt und kann keine Befehle mehr vom Kaseya Server empfangen.

So entfernen Sie die Option **Beenden** aus Agent-Menüs auf verwalteten Rechnern:

1. Wählen Sie eine oder mehrere Rechner-IDs aus.
2. Deaktivieren Sie das Kontrollkästchen **Beenden**.
3. Klicken Sie auf **Aktualisieren**.

Kontrollkästchen

- **Agent-Symbol aktivieren** – Aktivieren Sie dieses Kontrollkästchen, um das Agent-Symbol in der Systemablage des verwalteten Rechners anzuzeigen. Deaktivieren Sie dieses Kontrollkästchen, um das Agent-Symbol auszublenden und die Verwendung von Agent-Menü-Optionen zu verhindern.
- **Über<Agent>** – Aktivieren Sie dies, damit der Rechnerbenutzer auf diese Option klicken kann, um das Feld Info für den installierten Agent anzuzeigen. Die Standard-Optionsbezeichnung `Agent` kann angepasst werden.
- **<Administrator kontaktieren...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um entweder die Seite Portal-Zugang oder eine andere URL anzuzeigen. Die Standard-Optionsbezeichnung `Contact Administrator...` kann angepasst werden.
- **<URL Ihres Unternehmens...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die im entsprechenden URL-Feld angegebene URL anzuzeigen.
- **Fernsteuerung deaktivieren** – Aktvieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die Fernsteuerung auf dem verwalteten Rechner des Benutzers zu *deaktivieren*.
- **Konto festlegen...** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um seine Rechner-ID.Gruppen-ID.Organisations-ID anzuzeigen und die Kaseya Server-Adresse für die Agent-Anmeldung zu ändern. Die von Ihnen eingegebene, neue IP-Adrresse muss auf einen funktionierenden VSA verweisen. Ansonsten tritt die Änderung der IP-Adresse nicht in Kraft.
- **Aktualisieren** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer eine sofortige vollständige Anmeldung einleiten kann.
- **Beenden** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer den Agent-Dienst auf dem verwalteten Rechner beenden kann.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um Einstellungen des Agent-Menüs auf ausgewählte Rechner-IDs anzuwenden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem

Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

ACObSRx

Diese Spalte fasst die aktivierten Optionen des Agent-Menüs für eine Rechner-ID zusammen. **ÜBOtKAe** steht für die Tastaturkürzel, mit denen auf jede Option im Agent-Menü zugegriffen werden kann.

Ein Buchstabe deutet darauf hin, dass diese Option im Agent-Menü angezeigt wird. Ein "-" weist darauf hin, dass diese Menüoption nicht im Agent-Menü angezeigt wird.

Ü = **Ü**ber Agent

B = **B**enutzer kontaktieren

O = Startet die im URL-Feld angegebene URL. Der Agent zeigt den Text aus dem Feld links vom URL-Feld an.

t = Fernsteuerung deak**t**ivieren

K = **K**onto einrichten...

A = **A**ktualisieren

e = B**e**enden

Über den Titel

Der Text, der der Bezeichnung für die Option **Info** im Agent-Menü angehängt wurde. Wenn beispielsweise der Info-Titel `Agent` lautet, wird die Bezeichnung der Option **Über** als `About Agent` angezeigt.

Kontakttitel

Der Text, der im Agent-Menü als Kontakt für einen VSA-Benutzer angezeigt wird

Benutzerdefinierter Titel

Der Text, der im Agent-Menü als Kontakt für eine benutzerdefinierte URL angezeigt wird.

Kontakt-URL

Die URL, die angezeigt werden soll, wenn die Option `Contact Administrator...` vom Rechnerbenutzer ausgewählt wird. Die Standard-URL ist die Seite **Portalzugriff** *(siehe 54)*. Es kann eine andere URL eingegeben werden.

Benutzerdefinierte URL

Die URL, die angezeigt wird, wenn der Benutzer diese Option im Agent-Menü auswählt.

Check-in-Kontrolle

Agent > Agent konfigurieren > Check-in-Kontrolle

Auf der Seite **Check-in-Kontrolle** wird angegeben, wann und wo jeder Agent sich an einem Kaseya Server anmelden sollte. Sie können die primären und sekundären Kaseya Server-Namen/IP-Adressen für die Agent-Anmeldung, die von einem Agent zur Ausführung einer Aufgabe verbrauchte Bandbreite und den Anmeldungszeitraum festlegen.

- Der Agent meldet sich nur beim primären und nicht beim sekundären Server an, es sei denn, der primäre Server geht offline.
- Die primären und sekundären Kaseya Server-Werte und minimalen und maximalen Anmeldeperioden unterliegen den Richtlinien, die über System > Anmelderichtlinie eingerichtet wurden. Dies hindert Benutzer daran, Einstellungen auszuwählen, die den Servern, auf denen der Kaseya Server-Dienst ausgeführt wird, eine unnötige Last auferlegen.
- Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.
- Daten zur **Check-in-Kontrolle** können auch über die Registerkarte **Agent-Einstellungen** der Seiten **Live Connect** *(siehe 39)* und Rechnerübersicht gepflegt werden.

Beschränkungen des sekundären Servers

Legacy-Remote-Control-Funktionen werden über die primäre Kaseya Server-Adresse übermittelt. Wenn sich ein Agent bei der sekundären Kaseya Server-Adresse anmeldet, stellen Legacy-Remote-Control-Sitzungen keine Verbindung her, da sie an die falsche VSA-Übermittlungs-Serveradresse geleitet werden. Alle anderen Funktionen, einschließlich Kaseya Remote Control-Funktionen, werden unterstützt und vom sekundären Kaseya Server auf gleiche Weise wie die primäre Kaseya Server-Adresse geplant.

Agents zwischen Kaseya Server migrieren

Eventuell entscheiden Sie sich aus Gründen der Leistung oder Logistik, verwaltete Rechner auf einen neuen Kaseya Server zu migrieren. Dies kann jederzeit ausgeführt werden und es kommt nicht darauf an, ob die Agents gegenwärtig angemeldet sind.

1. Stellen Sie auf dem **Original**-Kaseya Server die **primäre** Kaseya Server-Einstellung so ein, dass sie auf die **neue** Kaseya Server-Adresse verweist.
2. Stellen Sie auf dem **Original**-Kaseya Server die **sekundäre** Kaseya Server-Einstellung so ein, dass sie auf die **Original**-Kaseya Server-Adresse verweist.
3. Stellen Sie auf dem **neuen** Kaseya Server sowohl die **primäre** als auch die **sekundäre** Kaseya Server-Einstellung so ein, dass sie auf den **neuen** Kaseya Server verweist.
4. Warten Sie darauf, dass sich alle Agents erfolgreich am **neuen** Kaseya Server anmelden. Zu diesem Zeitpunkt kann der **Original**-Kaseya Server offline gesetzt werden.

> **Hinweis:** Die neuesten Anweisungen zur Migration eines vorhandenen Kaseya Server auf einen neuen Rechner finden Sie im Abschnitt *Verschieben des Kaseya Server* in den aktuellen **Kaseya Server-Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/Install/index.asp#home.htm)*.

Port ändern, der von Agents für die Anmeldung am Kaseya Server verwendet wird

1. Stellen Sie den **primären** Port auf den **neuen** Port ein.
2. Stellen Sie den **sekundären** Port auf den **alten** Port ein.
3. Warten Sie darauf, dass die neuen Einstellungen für alle Agents wirksam werden.

4. Zeigen Sie die Seite System > Konfigurieren an. Geben Sie die neue Portnummer in das Bearbeitungsfeld **Serverport angeben, über den die Agents einchecken** ein und klicken Sie auf die Schaltfläche **Port ändern**.

> **Hinweis:** Falls Agents vor dem Wechsel des Kaseya Server noch nicht zum neuen Port migriert sind, müssen Sie den Port manuell auf den verwalteten Rechnern ändern. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol in der Systemablage, um das Agent-Menü auf dem verwalteten Rechner anzuzeigen, und wählen Sie die Option **Konto festlegen...** aus. Geben Sie die Serveradresse und den Serverport ein. Zum Beispiel: `192.168.1.7:1234`.

Primärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des primären Kaseya Server der Rechner-ID ein. Diese Einstellung wird in der Spalte **Primärer Kaseya Server** angezeigt.

Kaseya-Agents leiten sämtliche Kommunikationen mit dem Kaseya Server ein. Aus diesem Grund müssen sie immer in der Lage sein, den Domänennamen oder die IP-Adresse (Internet Protocol) zu erreichen, der/die dem Kaseya Server zugewiesen wurde. Wählen Sie eine IP-Adresse oder einen Domänennamen, der von allen gewünschten Netzwerken (sowohl im lokalen LAN und im Internet) aus aufgelöst werden kann.

> **Best Practices:** Obwohl eine öffentliche IP-Adresse verwendet werden kann, empfiehlt Kaseya die Verwendung eines **Domain Name Server (DNS)**-Namens für Kaseya Server. Dies wird als Vorsichtsmaßnahme empfohlen, falls die IP-Adresse geändert werden muss. Es ist einfacher, den DNS-Eintrag zu ändern, als verwaiste Agents umzuleiten.

Primärer Port

Geben Sie die Portnummer des primären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Primärer KServer** angezeigt.

> **Warnung:** Verwenden Sie KEINEN *Rechnernamen* für Ihren Server. Der Agent verwendet standardmäß WinSock-Aufrufe, um einen vollständig qualifizierten Hostnamen in eine IP-Adresse aufzulösen, die für alle Agent-Verbindungen verwendet wird. Der Rechnername wird von NETBIOS in eine IP-Adresse aufgelöst. Dies ist eventuell nicht auf jedem Rechner aktiviert. NETBIOS ist eine optionale letzte Methode, die Windows zum Auflösen eines Namens einsetzt. Daher werden nur vollständig qualifizierte Namen oder IP-Adressen unterstützt.

Sekundärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des sekundären Kaseya Server der Rechner-ID ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt. Der Agent meldet sich nur beim primären und nicht beim sekundären Server an, es sei denn, der primäre Server geht offline.

Sekundärer Port

Geben Sie die Portnummer des sekundären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt.

Check-in-Periode

Geben Sie das Zeitintervall ein, wie lange ein Agent warten soll, bevor er eine Schnellanmeldung mit dem Kaseya Server ausführt. Eine Anmeldung nimmt eine Prüfung im Hinblick auf eine neue Aktualisierung des Rechner-ID-Kontos vor. Wenn eine neue Aktualisierung von einem VSA-Benutzer eingestellt wurde, beginnt der Agent mit der Aufgabe bei der nächsten Anmeldung. Diese Einstellung wird in der Spalte **Anmeldezeitraum** angezeigt. Die minimal und maximal zulässigen Check-in-Perioden werden über System > Anmelderichtlinie eingerichtet.

Best Practices: Der Agent erhält eine ständige Verbindung mit dem Kaseya Server aufrecht. Daher wirken sich Schnellanmeldungszeiten nicht auf die Reaktionszeiten des Agents aus. Die Schnellanmeldungszeit legt die maximale Wartezeit fest, bevor eine ausgefallene Verbindung wiederhergestellt wird. Die Einrichtung der Schnellanmeldung der Rechner auf 30 Sekunden garantiert, dass sich jeder Agent innerhalb von 30 Sekunden von einer ausgefallenen Verbindung erholt. Dabei wird vorausgesetzt, dass die Verbindung erfolgreich ist.

An Kserver binden

Wenn as Kontrollkästchen aktiviert ist, ist der Agent an eine **eindeutige Kaseya Server-ID** gebunden. Gebundene Agents können erst dann einchecken, wenn die eindeutige Kaseya Server-ID, an die sie über "Agent > **Check-in-Kontrolle** *(siehe 48)*" gebunden wurden, der eindeutigen ID des Kaseya Server unter "System > Konfigurieren > **ID ändern**" entspricht. Dadurch wird das Spoofing der IP-Adresse durch Umleitung von Agent-Check-ins verhindert. Ein Schloss-symbol im Seitenbereich zeigt, dass der Agent gebunden ist. Um Agents zu *lösen*, wählen die Rechner-IDs aus, entfernen das Häkchen bei **An Kserver binden** und klicken auf **Aktualisieren**. Das Schloss-symbol wird die ausgewählten Rechner nicht mehr angezeigt.

Bandbreitendrosselung

Mit dieser Funktion beschränken Sie den Agent auf den Verbrauch einer Höchstmenge an Bandbreite im System. Standardmäßig teilt sich der Agent die Bandbreite mit allen anderen laufenden Anwendungen, sodass normalerweise keine Bandbreitendrosselung aktiviert werden muss. Deaktivieren Sie die Bandbreitendrosselung, indem Sie eine 0 eingeben.

Warnen, wenn mehrere Agents das gleiche Konto verwenden

Der Kaseya Server kann ermitteln, wenn mehr als ein Agent eine Verbindung mit dem Kaseya Server herstellt und dieselbe Rechner-ID.Gruppen-ID.Organisations-ID verwendet. Dieses Problem könnte durch das Installieren eines mit der Rechner-ID vorkonfigurierten Agent-Installationspakets auf mehr als einem Rechner verursacht werden. Markieren Sie dieses Kontrollkästchen, um jedes Mal, wenn Sie sich als Benutzer beim Kaseya Server anmelden, Benachrichtigungen über mehrere Agents zu erhalten, die das gleiche Konto verwenden.

Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist

Wenn Sie Rechner verwalten, die das gleiche LAN nutzen wie Ihr Kaseya Server, erhalten Sie möglicherweise diese Warnung. Standardgemäß verbinden sich alle Agents mit dem/der gleichen externen Namen/IP-Adresse zurück zum Kaseya Server. TCP/IP-Meldungen dieser Agents werden über Ihr internes LAN an Ihren Router und anschließend zurück zum Kaseya Server geleitet. Einige Router leiten internen Verkehr mehr schlecht als recht durch sich selbst zurück. Markieren Sie dieses Kontrollkästchen, um eine Meldung zu erhalten, wenn der Kaseya Server einen Agent im selben LAN ermittelt, der über den Router verbunden ist.

Hinweis: Agents im selben LAN wie der Kaseya Server sollten die gemeinsame interne IP-Adresse des Agents und des Kaseya Server angeben, die auf der Seite **Anmeldesteuerung** *(siehe 48)* festgelegt wurde.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um alle ausgewählten Rechner-IDs mit den vorher ausgewählten Optionen zu aktualisieren.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online

- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Arbeitsverzeichnis

Agent > Agent konfigurieren > Arbeitsverzeichnis

Auf der Seite **Arbeitsverzeichnis** wird ein Pfad zu einem Verzeichnis auf dem verwalteten Rechner eingestellt, das vom Agent zum Speichern der Arbeitsdateien verwendet wird.

Je nach der anliegenden Aufgabe verwendet der Agent mehrere zusätzliche Dateien. Der Server überträgt diese Dateien in ein Arbeitsverzeichnis, das vom Agent auf dem verwalteten Rechner verwendet wird. Bei ausgewählten Rechner-IDs können Sie das Standard-Arbeitsverzeichnis von `C:\kworking` in einen anderen Speicherort ändern.

> **Warnung: Löschen Sie keine Dateien und Ordner im Arbeitsverzeichnis.** Der Agent verwendet die im Arbeitsverzeichnis gespeicherten Daten, um verschiedene Aufgaben auszuführen.

Sie können dieses Verzeichnis in Sicherheitsprogrammen (z. B. Virenprüfprogramme) bestätigen, um zu verhindern, dass Vorgänge wie etwa die Fernsteuerung blockiert werden.

> **Hinweis:** Ein Arbeitsverzeichnis kann auch über die Registerkarte **Agent-Einstellungen** der Seiten Live-Connect und Rechnerübersicht gepflegt werden. Mithilfe des Befehls **getVariable()** in Agent-Verfahren kann in das Arbeitsverzeichnis geschrieben werden.

Übernehmen

Klicken Sie auf **Einrichten**, damit ausgewählte Rechner-IDs das vorher eingegebene Arbeitsverzeichnis verwenden.

Stellen Sie einen Pfad zum Verzeichnis her, das vom Agent für die Speicherung der Arbeitsdateien verwendet wird

Geben Sie den Pfad des Arbeitsverzeichnisses ein, das vom Agent auf dem verwalteten Rechner verwendet wird.

Als Systemstandard einstellen

Klicken Sie auf **Als Systemstandard einstellen**, um einen systemweiten Standard für das Agent-Arbeitsverzeichnis festzulegen. Diese Option wird nur für Masterrollenbenutzer angezeigt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Pfad für Arbeitsverzeichnis

Der Pfad des Arbeitsverzeichnisses, das dieser Rechner-ID zugewiesen wurde. Auf einem Apple OS X-System muss dem Pfad ein Schrägstrich vorangestellt werden, wenn er eine Leerstelle enthält. Zum Beispiel: `/tmp/name\ with\ three\ spaces`

Profil bearbeiten

Agent > Agent konfigurieren > Profil bearbeiten

Auf der Seite **Profil bearbeiten** werden Kontaktinformationen, die Sprache des Agent-Menüs auf dem Rechner des Benutzers und Anmerkungen zu jedem Rechner-ID-/Gruppen-ID-Konto gepflegt. Die Profilinformationen können an drei anderen Stellen gepflegt werden:

- Die Kontaktinformationen auf der Seite **Profil bearbeiten** können automatisch ausgefüllt werden, wenn über die Seite Agent > **Erstellen** *(siehe 34)* ein neues Konto erstellt wird.
- Sowohl VSA-Benutzer als auch Rechnerbenutzer können Kontaktinformationen über die Registerkarte Startseite > **Profil ändern** im Fenster Live-Connect oder **Portalzugriff** *(siehe 54)* ändern.
- Nur VSA-Benutzer können Anmerkungen und Kontaktinformationen auch über die Registerkarte **Agent-Einstellungen** der Seiten Live-Connect und Rechnerübersicht pflegen.

So ändern Sie die Einstellungen der Benutzerkonten:

1. Wählen Sie im Seitenbereich eine Rechner-ID aus.
2. Geben Sie die Informationen für **Anmerkungen**, **Admin-E-Mail**, **Kontaktname**, **Kontakt-E-Mail** und **Kontakt Telefon** ein.
3. Klicken Sie auf **Aktualisieren**.

Spezielle Anweisungen

Geben Sie Anmerkungen zu einem Rechner-ID-Konto ein. Hilfreiche Daten sind zum Beispiel Standort des Rechners, Rechnertyp, Firma oder sonstige Erkennungsdaten zum verwalteten Rechner. Diese

speziellen Anweisungen werden angezeigt, wenn Sie den Cursor über ein Agent-Statussymbol mit einem Zeichen bewegen. Im Fenster Schnellansicht wird der Text mit den **speziellen Anweisungen** unten im Fenster angezeigt.

Symbol-Abzeichen

Fügen Sie *Zeichen* zur unteren rechten Ecke des Agentstatussymbols hinzu, wie . Diese Zeichen werden überall angezeigt, wo das Agent-Symbol in der Benutzeroberfläche erscheint. Sie können beispielsweise einen Rechner mit einem -Zeichen versehen, um anzugeben, dass der Kunde einen Telefonanruf bekommen muss, bevor jemand an diesem Rechner arbeitet. Sie können einen Server auch mit einem -Zeichen markieren, damit dieser erst nach Betriebsschluss verwendet wird.

Wählen Sie auf der Seite Agent > **Profil bearbeiten** *(siehe 52)* mindestens einen Rechner aus. Klicken Sie anschließend auf den Link **Symbol-Abzeichen** oben auf der Seite und wählen Sie eines der verfügbaren Zeichen aus. Sie können eine Textnachricht mit **speziellen Anweisungen** für jedes Zeichen definieren. Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Zeichen ausgewählten Rechnern zuzuweisen.

Wenn Sie den Cursor über ein Agent-Statussymbol mit einem Zeichen bewegen, wird das Fenster Schnellansicht im Text mit den **speziellen Anweisungen** unten im Fenster angezeigt.

Tickets automatisch zuweisen

Weisen Sie automatisch ein Ticket zu dieser Rechner-ID zu, wenn der **Ticketing**-E-Mail-Reader oder ein **Service-Desk**-E-Mail-Reader eine E-Mail von der gleichen E-Mail-Adresse wie das Feld **Kontakt-E-Mail** von **Profil bearbeiten**. Gilt dann, wenn neue E-Mails in den **Ticketing**-E-Mail-Reader kommen, die sich nicht einer der E-Mail-Mapping zuordnen lassen, oder wie für **Service-Desk** im Abschnitt "Ticketverknüpfungen" des Themas **Registerkarte "Leseprogramme"** *(http://help.kaseya.com/webhelp/DE/KSD/9000000/index.asp#7560.htm)* in der Online-Hilfe beschrieben.

> **Hinweis:** Wenn mehrere Rechner-IDs dieselbe **Kontakt-E-Mail** haben, kann dieses Kontrollkästchen nur auf einem einzigen Rechner aktiviert sein.

Ansprechpartner

Geben Sie den Namen der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontaktname** angezeigt.

Kontakt-E-Mail

Geben Sie die E-Mail-Adresse der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-E-Mail** angezeigt.

Telefon

Geben Sie die Telefonnummer der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-Telefon** angezeigt.

E-Mail-Administrator

Geben Sie die E-Mail-Adresse ein, unter der dieser verwaltete Rechner Administrator-Support erhält. Diese Einstellunge wird in der Spalte **Admin-E-Mail** angezeigt.

Spracheinstellungen

Die in der Dropdown-Liste **Spracheinstellungen** ausgewählte Sprache legt die Sprache fest, die in einem **Agent-Menü** *(siehe 45)* auf einem verwalteten Rechner angezeigt wird. Die verfügbaren Sprachen werden von den über System > Voreinstellungen installierten Sprachpaketen bestimmt.

Rechnerrolle

Die Rechnerrolle, die auf ausgewählte Rechner-IDs angewendet wird. Rechnerrollen legen die

Funktionen für den **Portalzugriff** *(siehe 54)* fest, die dem Rechnerbenutzer zur Verfügung stehen.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um ausgewählte Rechner-IDs mit den vorher eingegebenen Profilinformationen zu aktualisieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Portalzugriff

Agent > Agent konfigurieren> Portalzugriff

Auf der Seite **Portalzugriff** werden der Anmeldename und das Kennwort nach Rechner-ID definiert, damit Live-Connect von einem Rechnerbenutzer *remote* verwendet werden kann. Eine von einem Rechnerbenutzer ausgeführte **Live-Connect**-Sitzung wird als **Portalzugriff** bezeichnet. Die über **Portalzugriff** angezeigten Funktionen werden auf der Seite System > Rechnerrollen > Zugriffsrechte festgelegt.

> **Hinweis:** Unter dem ersten Thema der Online-Hilfe können Sie eine **Live-Connect** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/DE_RCtools_R9.pdf#zoom=70&navpanes=0)*-PDF herunterladen.
>
> **Hinweis:** Lesen Sie **Ticketing für Portalzugriffbenutzer auf nicht unterstützten Browsern aktivieren** *(siehe 56)*.

Lokaler Zugriff auf den Portalzugriff

Rechnerbenutzer brauchen sich nicht lokal am **Portalzugriff** anmelden. Durch Klicken auf das Agent-Symbol in der Systemablage Ihres Rechners wird die **Portalzugriffs**-Sitzung ohne Anmeldung eingeleitet.

Remote Zugriff auf die Anmeldeseite des Portalzugriffs

Ein Rechnerbenutzer kann die Anmeldeseite des **Portalzugriffs** für seinen eigenen Rechner von einem

anderen Rechner wie folgt anzeigen:

1. Blättern Sie zur Seite `http://your_KServer_address/access/` und ersetzen Sie `your_KServer_address` durch den entsprechenden Ziel-Kaseya Server-Namen im URL-Text.

   Hinweis: Dies ist die gleiche Seite wie die, die VSA-Benutzer zur Anmeldung am VSA verwenden.

2. Melden Sie sich an, indem Sie den Benutzernamen und das Kennwort für den Rechner eingeben. Der Benutzername und das Kennwort werden über die Seite Agent > **Portalzugriff** festgelegt.

   Die Seite **Portalzugriff** wird angezeigt. Der Rechnerbenutzer kann auf jede Menüoption klicken, so als ob er von seinem eigenen verwalteten Rechner aus angemeldet wäre. Er kann auf die Menüoptionen **Desktop** oder **Dateiübertragung** klicken, um eine Remote Verbindung zu seinem eigenen Rechner einzuleiten, ein Ticket zu erstellen oder anzuzeigen oder einen Chat zu beginnen, wenn diese Optionen von der Rechnerrolle aktiviert wurden.

Benutzeranmeldungen neu aktivieren

Anmeldungen von Rechnerbenutzern folgen der gleichen Anmelderichtlinie wie VSA-Benutzeranmeldungen. Wenn ein Benutzer versucht, sich zu oft mit dem falschen Kennwort anzumelden, wird sein Konto automatisch deaktiviert. Sie können die Anmeldung neu aktivieren, indem Sie ein neues Kennwort festlegen oder darauf warten, dass die Deaktivierungszeit für das Konto verstrichen ist.

Portalzugriff anpassen

Portalzugriff-Sitzungen können über System > Anpassen > Live-Connect angepasst werden. Es können auch ein Logo, eine Startseite und Links zu anderen URLs hinzugefügt werden.

Login-Name

Geben Sie den **Anmeldenamen** ein, mit dem sich der Benutzer beim VSA anmelden muss, um Chat-Sitzungen einzuleiten, Tickets einzugeben oder anzuzeigen und/oder Fernzugriff auf seinen Rechner zu erhalten. Bei Anmeldenamen und Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Kennwörter müssen mindestens sechs Zeichen lang sein. Der **Anmeldename** wird standardmäßig als Rechner-ID.Gruppen-ID-Name übernommen.

Kennwort erstellen, Kennwort bestätigen

Definieren Sie ein Kennwort für die Anmeldung des Rechnerbenutzers. Kennwörter müssen aus mindestens 6 Zeichen bestehen. Der Rechnerbenutzer kann das Kennwort ändern, nachdem der VSA-Benutzer eins zugewiesen hat.

Anwenden

Klicken Sie auf **Anwenden**, um den Anmeldenamen und das Kennwort für den **Portalzugriff** auf die ausgewählte Rechner-ID anzuwenden.

Löschen

Entfernen Sie die Anmeldedaten für den **Portalzugriff** endgültig von der ausgewählten Rechner-ID.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Login-Name

Der dieser Rechner-ID zugewiesene Anmeldename für den **Portalzugriff**

Benutzer-Webanmeldung

Zeigt `Enabled` an, wenn dieser Rechner-ID ein Anmeldename und Kennwort für den **Portalzugriff**

zugewiesen wurden. Es zeigt an, dass sich ein Rechnerbenutzer über einen Webbrowser auf einem anderen Rechner *remote* bei der Seite **Portalzugriff** für seinen eigenen Rechner anmelden kann.

Ticketing für Portalzugriffbenutzer auf nicht unterstützten Browsern aktivieren.

Live-Connect und **Portalzugriff** werden auf bestimmten Browsern, die z.B. älter als IE8 oder Firefox 3.5 sind, nicht unterstützt. Rechnerbenutzer, die mit nicht unterstützten Browsern arbeiten müssen, können auf folgendem Weg Ticketing-Tickets erstellen und anzeigen:

1. Erstellen Sie eine eigene Rechnerrolle für Benutzer mit nicht unterstützten Browsern in System > Rechnerrollen. Erstellen Sie zum Beispiel eine Rechnerrolle `Tickets Only`.
2. Für die neue Rechnerrolle, die Sie soeben erstellt haben, deaktivieren Sie das Kontrollkästchen **Live-Connect** auf der Registerkarte System > Rechnerrollen > Zugriffsberechtigungen.
3. Weisen Sie Rechner mit nicht unterstützten Browsern dieser neuen Rechnerrolle zu.
4. Wenn die Rechnerbenutzer ihr Agent-Symbol anklicken, erscheint ein einziges **Ticketing**-Fenster anstelle des Fensters **Portalzugriff**.

> **Hinweis:** Wenn diese Option aktiviert ist, gilt sie für alle Benutzer, die den gleichen verwalteten Rechner verwenden.

Anmeldedaten eingeben

Agent > Agent konfigurieren > Anmeldedaten einstellen

Auf der Seite **Anmeldeinformationen einrichten** werden die erforderlichen Anmeldedaten registriert, damit ein Agent Aufgaben auf Benutzerebene auf einem verwalteten Rechner ausführen kann. Als Anmeldeinformationen bezeichnet man den Anmeldenamen und das Kennwort, die zur Authentifizierung des Zugriffs auf einen Rechner, ein Netzwerk oder eine andere Ressource durch einen Benutzer oder einen Prozess verwendet werden. Die meisten Agent-Aufgaben erfordern keine Anmeldeinformationen. Anmeldeinformationen sind insbesondere erforderlich oder es wird auf sie verwiesen bei:

- Patch-Management – Wenn Anmeldedaten für eine Rechner-ID definiert wurden, installiert **Patch-Management** alle neuen Patches unter Verwendung dieser Anmeldedaten. Daher sollte **Anmeldedaten einstellen** *(siehe 56)* immer *ein Benutzer mit Administratorrechten sein.*
- Patch-Status – Patch-Status setzt die Testergebnisse jedes Mal zurück, wenn **festgelegte Anmeldeinformationen** einer Rechner-ID geändert werden.
- Dateiquelle – Dateiquelle erfordert eventuell, dass festgelegte Anmeldeinformationen als Dateifreigabe für die Rechner-ID definiert werden.
- Patch-Meldung – Richten Sie eine Meldung ein, damit Sie benachrichtigt werden, wenn die Anmeldeinformationen einer Rechner-ID fehlen oder ungültig sind.
- Office-Quelle – Der Agent muss über Anmeldedaten verfügen, um auf den alternativen Office-Speicherort zuzugreifen, falls ein Patch installiert wird, ohne dass ein Benutzer am Rechner angemeldet ist.
- IF-THEN-ELSE – Der Befehl `useCredential()` im Agent-Verfahren-Editor erfordert zur erfolgreichen Ausführung, dass Anmeldedaten in **Anmeldedaten einrichten** definiert wurden.
- **Backup** > **Abbildspeicherort** *(http://help.kaseya.com/webhelp/DE/KSD/9000000/index.asp#7948.htm)*– Wenn in **Abbildspeicherort** ein UNC-Pfad angegeben wurde, müssen über **Anmeldedaten einrichten** Anmeldeinformationen definiert werden, die Zugriff auf diesen UNC-Pfad bereitstellen. Ohne die Anmeldedaten hat der Rechner *keinen* Zugriff auf den Abbildspeicherort und die Sicherung

schlägt fehl. Stellen Sie beim Angeben eines UNC-Pfads für eine Freigabe, auf die von einem Agent-Rechner zugegriffen wird – zum Beispiel `\\machinename\share` – sicher, dass die Berechtigung der Freigabe Lese-/Schreibzugriff unter Verwendung der Anmeldedaten für diesen Agent-Rechner in > **Anmeldedaten einstellen** *(siehe 56)* zulässt.

- **Ansichtdefinitionen** *(siehe 6)* – Enthält die Option **Rechner mit dem Anmeldestatus**, mit deren Hilfe Sie die Anzeige der Rechner-IDs auf jeder Agent-Seite nach ihrem Anmeldestatus filtern können.
- Desktop Management – Für die Installation des Clients für dieses Modul müssen Anmeldeinformationen definiert sein.

Leere Kennwörter

Leere Kennwörter können verwendet werden, wenn die **lokale Sicherheitsrichlinie** des verwalteten Rechners dies gestattet. Öffnen Sie auf dem verwalteten Rechner in "Verwaltung" das Tool "Lokale Sicherheitsrichtlinie". Navigieren Sie zu "Lokale Richtlinien – Sicherheitsoptionen". Suchen Sie nach einer Richtlinie namens `Accounts: Limit local account use of blank passwords to console logon only`: Die Standardeinstellung ist aktiviert. Wenn Sie sie in "deaktiviert" ändern, kann ein leeres Kennwort verwendet werden.

Benutzername

Geben Sie den Benutzernamen für die Anmeldeinformationen ein. Normalerweise ist dies ein Benutzerkonto.

Kennwort

Geben Sie das Kennwort ein, das mit dem oben genannten Benutzernamen verknüpft ist.

Domäne

Lokales Benutzerkonto – Wählen Sie diese Option aus, um Anmeldeinformationen für eine lokale Anmeldung an diesem Rechner ohne Verweis auf eine Domäne zu verwenden.

Aktuelle Domäne des Rechners verwenden – Erstellen Sie Anmeldeinformationen unter Verwendung des Namens der Domäne, deren Mitglied dieser Rechner ist. Dies wird vom letzten Audit bestimmt. **Alles markieren** erlaubt schnell und einfach einen gemeinsamen Benutzernamen / ein gemeinsames Kennwort auf mehreren Rechnern einzurichten, selbst wenn ausgewählte Rechner verschiedenen Domänen angehören.

Domäne angeben – Geben Sie den Domänennamen manuell an, der für diese Anmeldeinformationen verwendet werden soll.

Anwenden

Weisen Sie die Anmeldeinformationen allen markierten Rechner-IDs zu. Rechner-IDs mit zugewiesenen Anmeldeinformationen zeigen den Benutzernamen und die Domäne in den entsprechenden Tabellenspalten an.

Löschen

Entfernen Sie die Anmeldeinformationen von allen markierten Rechner-IDs.

Test

Klicken Sie auf **Test**, um zu überprüfen, ob Benutzername/Kennwort/Domänen-Anmeldedaten funktionieren, bevor Sie sie einer Rechner-ID zuweisen.

Abbrechen

Klicken Sie auf **Abbrechen**, um das Testen der Benutzername/Kennwort/Domänen-Anmeldedaten abzubrechen.

LAN-Cache

Agent > Agent konfigurieren > LAN-Cache

Die Seite **LAN-Cache** designiert einen Rechner so, dass er als Dateiquelle für andere Rechner auf dem gleichen LAN agiert. Wenn ein LAN-Cache aktiviert ist und ein Rechner im gleichen LAN zum ersten Mal einen Download vom Kaseya Server anfordert, werden die Dateien auf den LAN-Cache-Rechner heruntergeladen und dann auf den anfordernden Rechner kopiert. Ab dem Zeitpunkt muss die Datei nicht mehr vom Kaseya Server heruntergeladen werden. Andere Rechner – auf dem gleichen LAN mit dem gleichen LAN-Cache – kopieren die Datei aus dem LAN-Cache-Rechner. Dadurch werden die Zustellung an mehrere Rechner im gleichen LAN beschleunigt und Probleme mit der Netzwerkbandbreite reduziert.

Hintergrund

LAN-Cache konfiguriert eine Dateiquelle wie folgt:

- Erstellt automatisch ein lokales Administrator- oder Domänen-Administratorkonto oder ermöglicht Ihnen, die Anmeldedaten für einen vorhandenen Domänen-Administrator manuell anzugeben. Erstellte Konten erhalten einen eindeutigen Namen (`FSAdminxxxxxxxxx`, wobei `x` eine Ziffer ist) mit einem automatisch generierten starken Kennwort. Das generierte Kennwort enthält 15 zufällig ausgewählte Zeichen, davon mindestens eines der folgenden Zeichen:
  - Großbuchstaben
  - Kleinbuchstaben
  - Zahlen (0–9)
  - Nicht-alphanumerische Zeichen
- Sobald das Kennwort erstellt wurde, wird es mit dem Adminnamen verglichen, um sicherzustellen, dass keine zwei Zeichenkombinationen im Kennwort mit zwei Zeichenkombinationen im Adminnamen übereinstimmen. Durch diese Logik wird sichergestellt, dass die generierten Kennwörter jeder Komplexitätslogik für Windows-Kennwörter entsprechen.
- Die Anmeldedaten für das Konto werden mit diesem LAN-Cache innerhalb von Kaseya verbunden und bei Bedarf anstatt von zugeordneten Agent-Anmeldedaten verwendet. *LAN-Cache erfordert und unterstützt nicht die Verwendung der auf der Seite "Anmeldedaten erstellen" angegebenen Anmeldedaten.*
- Erstellen des angegebenen Kundenfreigabeverzeichnisses auf dem angegebenen festen Laufwerk, das als Windows-Verwaltungsfreigabe konfiguriert ist. Das Verzeichnis und die Freigabe werden erstellt, ohne dass die Seite **LAN-Cache** verlassen werden muss. Das für den LAN-Cache angegebene Verzeichnis ist ausschließlich für die Kundenverwendung gedacht. *Kaseya verwendet dieses vom Kunden angegebene Verzeichnis/diese Freigabe nie.*
- Erstellen eines speziellen Kaseya-Verzeichnisses – immer `VSAFileShare` als Unterverzeichnis unter dem Kundenverzeichnis – auf dem angegebenen festen Laufwerk, das als Windows-Verwaltungsfreigabe konfiguriert ist.

Verfahren – Allgemein

1. Wählen Sie einen LAN-Cache-Rechner.
2. Weisen Sie Rechner über die Seite **LAN-Cache zuweisen** *(siehe 60)* dem LAN-Cache zu.

Verfahren – Für writeFile()- und getURL()-Schritte in Agent-Verfahren

Mit diesen Befehlen können Dateien von einem **LAN-Cache** anstatt von einem VSA oder einer URL heruntergeladen werden. Die Dateien müssen größer als 4 kB sein.

1. Wählen Sie einen LAN-Cache-Rechner.
2. Weisen Sie Rechner über die Seite **LAN-Cache zuweisen** *(siehe 60)* dem LAN-Cache zu.
3. Laden Sie *nur beim writeFile()-Befehl* die Dateien hoch, die Sie auf zugeordnete Rechner auf den Kaseya Server mit dem Ordner Agent-Verfahren > Verfahren verwalten > Planen/Erstellen >

Dateien verwalten > *Gemeinsam genutzt* herunterladen möchten. Die Dateien müssen größer als 4 kB sein.

4. Erstellen und führen Sie ein Agent-Verfahren aus, das einen writeFile()- oder getURL()-Schritt enthält.
    - Wenn ein Agent den Schritt **writeFile()** oder **getURL()** eines Agent-Verfahrens zum ersten Mal ausführt, wird die Datei vom KServer oder der URL heruntergeladen und dann wird der zugeordnete LAN-Cache mit der Datei aktualisiert.
    - Für nachfolgende Anforderungen für die gleiche Datei von einem beliebigen Agent wird die Datei vom LAN-Cache und nicht von ihrer ursprünglichen Quelle heruntergeladen.
    - Um den Caching-Mechanismus vollständig nutzen zu können, führen Sie zuerst das Agent-Verfahren aus, das die Datei auf einen Agent verweist. Nachdem dieser Agent die Datei in den zugeordneten LAN-Cache hochgeladen hat, führen Sie dieses Verfahren mit anderen Agents aus, die dem gleichen LAN-Cache zugeordnet sind.

Aktionen

- **LAN-Cache hinzufügen** – Gibt einen LAN-Cache auf einem ausgewählten Rechner an.
    - **1. LAN-Cache-Name** – Geben Sie einen Namen auf dem LAN-Cache an, wie er in **LAN-Cache zuordnen** angezeigt wird.
    - **2. Verzeichnisname** – Geben Sie nur den Namen des Verzeichnisses an, ohne den Namen des Rechners oder den Laufwerksbuchstaben anzugeben. Das Verzeichnis muss nicht bereits vorhanden sein. Der LAN-Cache erstellt das Verzeichnis und die erforderlichen Freigabeeinstellungen für Sie.
    - **3. Wählen Sie die UNC-Servernamenauflösung** – **Verwenden Sie den Computernamen** oder die **Computer-IP-Adresse**. Gibt das für den Zugriff auf die Freigabe verwendete UNC-Namenauflösungsformat an. Beispiel: `\\computername\sharename$` oder `\\10.10.10.118\sharename$`.

      > **Hinweis:** Der nächste Schritt, die Auswahl des Anmeldetypen, wird nicht angezeigt, wenn die Option System > Standardeinstellung > **LAN-Cache – Automatisch erstellte Administrator-Anmeldedaten verwenden** auf "Ja" gesetzt ist.

    - **4. Wählen Sie den zu verwendenden Typ der LAN-Cache-Administrator-Anmeldedaten aus.**
        - ✓ **Automatisch erstellte Administrator-Anmeldedaten verwenden** – Wenn diese Option aktiviert ist, werden Administrator-Anmeldedaten für Sie erstellt, wenn der LAN-Cache erstellt wird. Es werden lokale Administrator-Anmeldedaten erstellt, es sei denn, der Rechner ist ein Domain-Controller. Wenn der Rechner ein Domain-Controller ist, werden Domänen-Administratoranmeldedaten erstellt.
        - ✓ **Vorhandene Domänen-Administratoranmeldedaten verwenden** – Wenn diese Option aktiviert ist, geben Sie die Domäne, den Benutzernamen und das Kennwort vorhandener Domänen-Anmeldedaten ein. Die Domänen-Anmeldedaten werden nicht erstellt.
    - **5. Wählen Sie ein festes Laufwerk aus, auf dem der LAN-Cache erstellt wird.** – Wählen Sie das Laufwerk aus, auf dem die Freigabe erstellt wird.
- **LAN-Cache entfernen** – Entfernt den LAN-Cache aus einem ausgewählten Rechner.
- **Ausstehendes löschen** – Storniert die ausstehende Erstellung eines LAN-Cache auf einem ausgewählten Rechner.
- **Generierte Cache-Anmeldedaten testen** – Klicken Sie auf diese Option, um die von einem ausgewählten Rechner verwendeten Anmeldedaten zu testen. Das Ergebnis wird in der Spalte **Teststatus der Anmeldedaten** angezeigt.

Spalten

- **(Check-in-Symbol) –** Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Cache-Name** – Der Name des LAN-Cache, wie mit dem VSA angezeigt.
- **Cache-Pfad** – Der für den LAN-Cache angegebene Pfad.
- **Cache-UNC** – Der für die Lokalisierung des LAN-Cache im Netzwerk verwendete UNC.
- **Cache erstellt** – Datum/Uhrzeit, an dem bzw. zu der der LAN-Cache erstellt wurde.
- **Cache-Administrator** – Das für den Zugriff auf den LAN-Cache verwendete Administratorkonto.
- **Teststatus der Anmeldedaten** – Zeigt die Ergebnisse der Tests der Administrator-Kontoanmeldedaten an, die für den Zugriff auf den LAN-Cache verwendet werden. Anmeldedaten können über die Schaltfläche **Generierte Cache-Anmeldedaten testen** oben auf der Seite getestet werden.

LAN-Cache zuweisen

Agent > Agent konfigurieren > LAN-Cache zuweisen

Auf der Seite **LAN-Cache zuweisen** werden Rechner einem ausgewählten **LAN-Cache** *(siehe 58)*-Rechner zugewiesen bzw. daraus entfernt.

Aktionen

- **Zuweisen** – Weist einen aus der Dropdown-Liste ausgewählten LAN-Cache ausgewählten Rechnern zu.
- **Zuweisen aufheben** – Hebt die Zuweisung eines LAN-Cache zu ausgewählten Rechnern auf.
- **Ausstehendes löschen** – Storniert die ausstehende Zuweisung eines LAN-Cache zu einem ausgewählten Rechner.
- **Generierte Cache-Anmeldedaten testen** – Klicken Sie auf diese Option, um die von einem ausgewählten Rechner verwendeten Anmeldedaten zu testen. Das Ergebnis wird in der Spalte **Teststatus der Anmeldedaten** angezeigt.

Spalten

- **Alle auswählen/Alle abwählen** – Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Zugewiesener LAN-Cache** – Zeigt den LAN-Cache an, dem ein Rechner zugewiesen ist.
- **Zugewiesen** – Das Datum/die Uhrzeit, an dem ein Rechner einem LAN-Cache zugewiesen wurde.
- **Teststatus** – **Test Status der Anmeldedaten** – Zeigt die Ergebnisse der Tests der Administrator-Kontoanmeldedaten an, die für den Zugriff auf den LAN-Cache verwendet werden. Anmeldedaten können über die Schaltfläche **Generierte Cache-Anmeldedaten testen** oben auf der Seite getestet werden.

Agent aktualisieren

Agent > Version aufrüsten > Agent aktualisieren

Auf der Seite **Agent aktualisieren** wird geplant, verwaltete Rechner mit der neuesten Version der Agent-Software beider nächsten Anmeldung des Agents zu aktualisieren. Die für jeden Agent definierten Agent-Einstellungen werden durch diese Aktualisierung nicht geändert.

> **Hinweis:** Alle für die Überwachung verwendeten Agents müssen über die Seite Agent > Agent aktualisieren aktualisiert werden.

Agent aktualisieren

Klicken Sie auf **Agent aktualisieren**, um die Aktualisierung ausgewählter Rechner zu planen.

Beim Login daran erinnern, wenn Agents ein Update benötigen

Wenn dies markiert ist, wird bei der Anmeldung von VSA-Benutzern ein Popup-Fenster angezeigt, wenn verwaltete Rechner unter ihrer Kontrolle mit der letzten Version der Agent-Software aktualisiert werden müssen. Diese Erinnerungsmeldung wird nur angezeigt, wenn mindestens ein Agent innerhalb des Scopes des VSA-Benutzers aktualisiert werden muss. Benutzer können diese Funktion zum Zeitpunkt der Anmeldung deaktivieren und durch Markieren dieses Kontrollkästchens erneut aktivieren.

Update erzwingen, selbst wenn Agent-Version x.x.x.x. ist

Wenn dies aktiviert ist, werden die für die Aktualisierung ausgewählten Rechner mit neuen Dateien aktualisiert, die die Agent-Dateien auf dem verwalteten Rechner ersetzen, selbst wenn die Agent-Version gegenwärtig aktuell ist. Es wird eine "saubere" Installation der Agent-Dateien ausgeführt.

Nach der Aktualisierung über <Agent-Verfahren auswählen> Agent-Verrfahren ausführen

Wählen Sie ein Agent-Verfahren aus, das sofort nach Abschluss der Fertigstellung eines Agents ausgeführt werden soll. Mit dieser Funktion können Sie Anpassungen erneut auf einen Agent anwenden, die eventuell nach der Agent-Aktualisierung verloren gehen. Normalerweise umfassen diese Anpassungen das Ausblenden oder Umbenennen von Agent-Bezeichnern auf verwalteten Rechnern, damit Benutzer nicht erkennen, dass der Agent überhaupt installiert ist.

Update abbrechen

Klicken Sie auf **Update abbrechen**, um eine anstehende Aktualisierung auf ausgewählten verwalteten Rechnern abzubrechen.

Herunterladen des Live Connect-Plugin-Installationsprogramms für Windows-Browser

Bei allen Versionen von Windows, die von Live Connect unterstützt werden, wird durch Klicken auf diesen Link ein eigenständiges Installationsprogramm auf den lokalen Rechner des VSA-Benutzers heruntergeladen. Das Installationsprogramm installiert den Live Connect-Plugin Manager und alle Live Connect-Plugins für Chrome, Firefox und Internet Explorer.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits

- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Agentversion

Die Version der Agent-Software, die auf dem verwalteten Rechner ausgeführt wird. Versionsnummern in rot deuten darauf hin, dass die Version auf dem Agent-Rechner nicht dieselbe wie die aktuellste verfügbare Version ist.

Agent-Verfahren aktualisieren

Dies ist das Agent-Verfahren, das bei der Aktualisierung des Agents ausgeführt werden soll.

Letztes Update

Das Datum, an dem der Agent zuletzt auf dem verwalteten Rechner aktualisiert wurde. Da der Server auf einen Check-in des verwalteten Rechners warten muss (wie in Agent > **Check-in-Kontrolle** *(siehe 48)* angegeben), wird `Pending` in der Spalte **Letztes Update** angezeigt, bis der nächste Check-in eintritt.

Dateizugriff

Agent > Schutz > Dateizugriff

Über die Seite **Dateizugriff** kann der unautorisierte Zugriff auf Dateien auf verwalteten Rechnern durch Rogue-Anwendungen oder Benutzer verhindert werden. Jeder Anwendung kann der Zugriff auf die Datei gewährt oder verweigert werden.

> **Hinweis:** Sie können auch den Betriebssystemzugriff auf die geschützte Datei blockieren, indem Sie den Zugriff auf `explorer.exe` und/oder `cmd.exe` blockieren. Dadurch wird verhindert, dass die Datei umbenannt, verschoben oder gelöscht wird und damit jede Verfälschung der Datei unterbunden wird.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 29)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 62)*, **Netzwerkzugriff** *(siehe 64)* und **Anwendungsblocker** *(siehe 67)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

Blockieren

Wenn Sie den unautorisierten Zugriff auf eine Datei durch Rogue-Anwendungen verhindern wollen, geben Sie den Dateinamen ein und klicken Sie auf die Schaltfläche **Blockieren** . Dadurch wird das Popup-Fenster **Dateizugriff** eingeblendet.

In diesem Dialog kann der Benutzer zwischen folgenden Optionen wählen:

- **Dateiname für Zugriffskontrolle** – Geben Sie den **Dateinamen und/oder einen Teil des vollständigen Pfads** ein. Wenn Sie beispielsweise den Dateinamen `protectme.doc` zu der Liste hinzufügen, werden alle Vorkommnisse von `protectme.doc` in allen Verzeichnissen und auf jedem Laufwerk geschützt. Durch Hinzufügen von `myfolder\protectme.doc` werden alle Vorkommnisse der Datei in allen Verzeichnissen namens `myfolder` geschützt.
- **Neu** – Fügen Sie eine neue Anwendung zu der Zugriffsliste hinzu. Sie können die Anwendungen manuell eingeben oder mithilfe der Schaltfläche **Suchen...** einen Anwendungsnamen auswählen.
- **Entfernen** – Entfernen Sie eine Anwendung aus der Zugriffsliste.
- **Suchen** – Wählen Sie eine Rechner-ID aus, um die Liste der auf dieser Rechner-ID installierten Anwendungen zu durchsuchen, und wählen Sie anschließend einen Anwendungsnamen aus. Diese Liste basiert auf der letzten Inventarisierung, die für diese Rechner-ID durchgeführt wurde. Sie durchsuchen nicht wirklich den verwalteten Rechner.
- **Benutzer fragen, die nicht aufgelisteten freizugeben** – Damit wird dem Benutzer die Möglichkeit gegeben, den Zugriff auf die Datei auf Anwendungsbasis jedes Mal zu gewähren oder zu verweigern, wenn eine neue Anwendung versucht, auf diese Datei zuzugreifen. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen.
- **Alle nicht aufgelisteten ablehnen** – Blockiert alle Anwendungen vom Zugriff auf die Datei. Wählen Sie diese Option, wenn Sie sich nicht sicher sind, für welche Dateien Zugriff benötigt wird und für welche nicht.

Entsperren

Entfernen Sie eine Anwendung aus der Schutzliste, indem Sie auf die Schaltfläche **Entsperren** klicken. Dadurch wird ein neues Dialogfeld geöffnet, in dem alle geschützten Dateien für die ausgewählten Rechner-IDs ausgewählt werden. Sie können Dateien von dem ausgewählten Rechner oder von allen Rechnern mit diesem Dateipfad entfernen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Dateiname

Dateiname der zu blockierenden Datei. Klicken Sie auf das Bearbeitungssymbol neben einem Dateinamen, um die Dateizugriffsberechtigungen für diesen Dateinamen zu ändern.

Bestätigte Anwendungen

Hier werden die Anwendungen aufgelistet, für die der Zugriff auf die Datei auf dieser Rechner-ID bestätigt wurde.

Benutzer um Bestätigung bitten

Wenn diese Option aktiviert ist, wird der Benutzer einer Rechner-ID gefragt, ob er den Dateizugriff bestätigen will, wenn eine nicht zugelassene Anwendung versucht, auf die Datei zuzugreifen.

Netzwerkzugriff

Agent > Schutz > Netzwerkzugriff

Über die Seite **Netzwerkzugriff** können Sie den **TCP/IP-Protokoll-basierten Netzwerkzugriff** auf Anwendungsbasis bestätigen oder verweigern. Benutzer können ebenfalls benachrichtigt werden, wenn nicht eine aufgelistete Anwendung auf das Netzwerk zugreift, und dieser Anwendung den Netzwerkzugriff bestätigen oder verweigern. Über diese Funktion wird in der Regel der Zugriff auf interne und externe *Internet*-Sites gesteuert. Dies kann jedoch auch internen LAN-Verkehr, der das TCP/IP-Protokoll verwendet, einschließen.

Treiber

Diese Funktion erfordert, dass der Treiber *aktiviert*wird, den Netzwerkzugriff zu blockieren und die Bandbreitenstatistiken des Netzwerks zu überwachen. Dieser Treiber ist standardmäßig *deaktiviert*. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*

Hinweis: Um festzustellen, welchen Anwendungen der Netzwerkzugriff bestätigt oder verweigert werden soll, zeigen Sie über den Bericht Netzwerkstatistiken die Netzwerkbandbreitennutzung während eines bestimmten Zeitraums an. Klicken Sie auf die Datenpunkte des Diagramms, um weitere Details anzuzeigen und die Top-Verbraucher von Bandbreite zu identifizieren. Stellen Sie fest, welche Anwendung und welcher Rechner zu einem gegebenen Zeitpunkt Bandbreite verbraucht.

Warnung: Anwendungen, die den Windows TCP/IP-Stapel nicht auf normale Weise verwenden, können Konflikte mit dem Treiber verursachen, der zum Erfassen von Informationen und Blockieren des Zugriffs verwendet wird. Dies gilt insbesondere für ältere Anwendungen.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 29)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 62)*, **Netzwerkzugriff** *(siehe 64)* und **Anwendungsblocker** *(siehe 67)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

So bestätigen oder verweigern Sie den Netzwerkzugriff für eine oder mehrere Anwendungen

1. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Rechner-IDs in der Spalte **Rechner.Gruppen-ID**.
2. Klicken Sie auf den Link einer *beliebigen* Rechner-ID in der Spalte **Rechner.Gruppen-ID**. Dies braucht nicht unbedingt die Rechner-ID zu sein, die Sie markiert haben. Dadurch wird das Popup-Fenster **Anwendungsliste** mit allen auf dieser Rechner-ID installierten Anwendungen eingeblendet. Diese Liste basiert auf der letzten Inventarisierung, die für diese Rechner-ID durchgeführt wurde.

3. Da die im Fenster **Anwendungsliste** angezeigte Liste sehr umfangreich sein kann, sollten Sie sie durch Klicken auf **Filter** filtern und so die Anzeige der Dateien besser steuern.
4. Aktivieren Sie die Kontrollkästchen neben dem Namen der Anwendung, der Sie Netzwerkzugriff bestätigen oder verweigern möchten.
5. Sie können auch Anwendungsnamen in das Bearbeitungsfeld **Anwendungen, die bei Audit nicht gefunden wurden, hier hinzufügen** eingeben, um nicht aufgelistete Anwendungen zu identifizieren.
6. Klicken Sie auf die Schaltfläche **Auswählen**, um Ihre Auswahlen zu bestätigen und das Fenster **Anwendungsliste** zu schließen. Die ausgewählten Anwendungen werden jetzt am Anfang der Seite angezeigt.
7. Klicken Sie auf **Anwendungen bestätigen** oder **Anwendungen ablehnen**. Die im Fenster **Anwendungsliste** ausgewählten Anwendungen werden zur Spalte **Bestätigte/Abgelehnte Anwendungen** hinzugefügt.

So entfernen Sie die Einstellungen für Bestätigung und Ablehnung für eine oder mehrere Rechner-IDs

1. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Rechner-IDs in der Spalte **Rechner.Gruppen-ID**.
2. Klicken Sie auf die Schaltfläche **Anwendungen entfernen**.

Optionen für Netzwerkzugriff

- **Benutzer benachrichtigen, wenn Anwendung geblockt ist** – Benutzer benachrichtigen, wenn eine geblockte Anwendung auf das Netzwerk zugreifen will. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen. Auf diese Weise können Sie sehen, welche Anwendungen auf Ihrem System auf das Netzwerk zugreifen und wann. Der Rechnerbenutzer ist aufgefordert eine von vier Antworten zu wählen, wenn eine Anwendung geblockt ist:
  - **Immer** – Gewährt der Anwendung unbegrenzt den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
  - **Ja** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung gewährt. Die Benutzer werden erneut aufgefordert.
  - **Nein** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung verweigert. Die Benutzer werden erneut aufgefordert.
  - **Nie** – Verweigert der Anwendung immer den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
- **Treiber bei nächstem Neustart aktivieren/deaktivieren** – den Netzwerkzugriff-Protection-Treiber für einen Agent **Aktivieren/Deaktivieren**. Anwendungen, die den Windows TCP/IP-Stapel nicht auf normale Weise verwenden, können Konflikte mit diesem Treiber verursachen. Dies gilt insbesondere für ältere Anwendungen. **Der Agent kann keine Netzwerkstatistiken überwachen oder den Netzwerkzugriff blockieren, wenn der Treiber deaktiviert ist.** *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*
- **Nicht gelistete Aktion anwenden** – Bei einer nicht gelisteten Anwendung handelt es sich um eine Anwendung, für die der Zugriff auf das Netzwerk nicht ausdrücklich gewährt oder verweigert wurde. Geben Sie an, was unternommen werden soll, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Benutzer bitten, die nicht gelisteten freizugeben** – Ein Bestätigungsdialogfeld wird angezeigt, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Alle nicht gelisteten freigeben** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk gewährt.
  - **Alle nicht gelisteten ablehnen** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk verweigert, und die Anwendung wird auf dem verwalteten Rechner geschlossen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Benutzer benachrichtigen

Ein grünes Häkchen in der Spalte **Benutzer benachrichtigen** weist darauf hin, dass der Benutzer des verwalteten Rechners benachrichtigt wird, wenn eine Anwendung versucht, auf das Netzwerk zuzugreifen, der der Netzwerkzugriff verweigert wurde.

So benachrichtigen Sie den Benutzer, wenn eine Anwendung abgelehnt wurde:

1. Wählen Sie die Rechner-IDs aus.
2. Klicken Sie auf die Schaltfläche **Aktivieren** für **Benutzer benachrichtigen, wenn die Anwendung blockiert ist**.

So entfernen Sie diese Benachrichtigung:

1. Wählen Sie die Rechner-IDs aus, für die in der Spalte **Benachrichtigen** ein grünes Häkchen angezeigt wird.
2. Klicken Sie auf die Schaltfläche **Deaktivieren** für **Benutzer benachrichtigen, wenn die Anwendung blockiert ist**.

Treiber aktivieren

Identifiziert auf Rechner-ID-Basis, für welche Rechner der Netzwerkschutztreiber aktiviert wurde oder nicht. *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*

Nicht aufgelistete Aktion

Zeigt die **nicht gelistete Aktion** an, die ausgeführt werden soll, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen. Siehe **Nicht gelistete Aktion anwenden** weiter oben.

Bestätigte Anwendungen / Lehnt Anwendungen ab / Anwendungen entfernen / Alle entfernen

Diese Einstellungen können erst angewendet werden, wenn der Treiber aktiviert ist.

- Bestätigte Anwendungen werden in der ersten Zeile gelistet.
- Abgelehnte Anwendungen werden in der zweiten Zeile gelistet.

- Falls das Optionsfeld **Alle nicht gelisteten bestätigen** ausgewählt ist und auf eine Rechner-ID angewendet wurde, wird die Liste der bestätigten Anwendungen durch den Ausdruck `Approve All Unlisted` ersetzt.
- Falls das Optionsfeld **Alle nicht aufgelisteten ablehnen** ausgewählt ist und auf eine Rechner-ID angewendet wurde, wird die Liste der bestätigten Anwendungen durch den Ausdruck `Deny All Unlisted` ersetzt.
- Klicken Sie auf **Anwendungen entfernen**, um ausgewählte Anwendungen von ausgewählten Rechner zu entfernen.
- Klicken Sie auf **Anwendungen entfernen**, um ausgewählte Anwendungen von ausgewählten Rechner zu entfernen.

Anwendungsblocker

Agent > Schutz > Anwendungsblocker

Über die Seite **Anwendungsblocker** kann verhindert werden, dass beliebige Anwendungen auf einer Rechner-ID ausgeführt werden. Blockierte Anwendungen können weder umbenannt noch verschoben oder vom System gelöscht werden. **Dateizugriff** *(siehe 62)* kann auch Anwendungen blockieren, **Anwendungsblocker** kann jedoch schneller konfiguriert werden, wenn Sie Anwendungen einfach nur blockieren bzw. die Blockierung aufheben möchten.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 29)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 62)*, **Netzwerkzugriff** *(siehe 64)* und **Anwendungsblocker** *(siehe 67)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

Blockieren

So blockieren Sie das Ausführen einer Anwendung auf einem Rechner:

1. Wählen Sie eine oder mehrere Rechner-IDs aus. Nur Rechner-IDs, die aktuell dem **Rechner-ID/Gruppen-ID-Filter** *(siehe 5)* entsprechen, werden angezeigt.
2. Geben Sie den Dateinamen der Anwendung in das Bearbeitungsfeld ein.

   Die Anwendung kann **durch ihren Dateinamen und/oder einen Teil des vollständigen Pfads referenziert werden**. Beispiel: Durch Hinzufügen einer Anwendung namens `blockme.exe` zu der Liste wird die Ausführung aller Vorkommnisse von `blockme.exe` in jedem Verzeichnis und auf jedem Laufwerk verhindert. Wenn Sie `myfolder\blockme.exe` hinzufügen, wird die Ausführung aller Vorkommnisse der Anwendung in allen Verzeichnissen namens `myfolder` verhindert.
3. Klicken Sie auf die Schaltfläche **Blockieren** .
4. Die blockierte Anwendung wird in der Spalte **Anwendung** neben den ausgewählten Rechner-IDs angezeigt.

Entsperren

So entsperren Sie eine Anwendung in der Liste der blockierten Anwendungen:

1. Wählen Sie eine oder mehrere Rechner-IDs aus, die blockierte Anwendungen in der Spalte **Anwendung** aufführen.
2. Klicken Sie auf die Schaltfläche **Entsperren**. Ein Popup-Fenster **Dateizugriff** wird geöffnet, in dem alle blockierten Anwendungen für die ausgewählten Rechner-IDs aufgelistet sind.
3. Klicken Sie auf eine oder mehrere blockierte Anwendungen.
4. Klicken Sie auf die Schaltfläche **Entsperren**. Das Fenster wird geschlossen.
5. Die blockierte Anwendung wird nicht länger in der Spalte **Anwendung** neben den ausgewählten Rechner-IDs angezeigt.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 5)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Anwendung

Der Dateiname der blockierten Anwendung.

Inhaltsverzeichnis

A

B

C

D

E

G

I

K

L

M

N

P

R

T

U

Z